Government Cloud Computing Strategies:

Management of information risk and impact on concepts and practices of information management

Peter Bisley

Submitted to the School of Information Management, Victoria University of Wellington
in partial fulfilment of the requirements for the degree of Master of Information Studies

November 2013

Abstract

Research Problem

The objective of this research is to investigate the extent to which the government cloud computing strategies of New Zealand, Australia, the United States, the United Kingdom, Canada and Ireland are supported by defined processes for considering the information risks of shifting to cloud computing, and assessing the impact of these approaches on concepts and practices of information management.

Methodology

The study undertook a qualitative analysis of published policies, strategies and guidance documents published by regulatory agencies within the target jurisdictions, investigating these documents for evidence of a process to assess and manage information risks.

Results

The study provides an assessment of the adequacy of governments' guidance frameworks in preparing government organisations to properly assess the risks, opportunities, and necessary controls for information in a cloud service.

Implications

The gaps in guidance demonstrated by the study identify opportunities for a more rigorous assessments of the effectiveness of information management controls and privacy safeguards implemented by government organisations, and points to characteristics which could be assessed against in more specific case studies.

Keywords

Information management, information risk, offshore computing, cloud computing, cloud services, as-a-service, risk management

Contents

Problem definition and context

Technology commentators expect that governments around the world will increasingly adopt cloud services in the course of replacing obsolete information technology and expanding their delivery of digital services. Research has noted this is due to the two converging trends: the increasing pace of automation and digitisation of processes within the public sector, and the maturation of cloud computing services providers in providing “ubiquitous, on-demand access to computing resources” (Irion, 2012, p 40).

Cloud computing is frequently associated with new and difficult-to-assess risks. While it is an understandable reaction to risks to withdraw from a risk-prone activity, cloud technology has already attracted significant interest from governments. With the literature suggesting that wide-scale adoption of cloud computing technologies by governments a near certainty, it is important to not only recognize the risks associated with these technologies, but to “create a strategy that allows organizations to better manage and mitigate these risks” (Paquette, Jaeger & Wilson, 2010, p 248). The objective of this research is to investigate the extent to which the government cloud computing strategies of New Zealand, Australia, the United States, the United Kingdom, Canada and Ireland are supported by defined processes for considering the information risks of shifting to cloud computing, and assessing the impact of these approaches on concepts and practices of information management. For the purposes of this study information management is defined as the organisational strategies, business processes, and technology used for controlling and managing the information an organisation creates and receives in the course of its official business.

This study investigates the frameworks by which government cloud computing strategies are being implemented, conducting a comparative analysis of the guidance issued by six jurisdictions with respect to the management of information and information-related risks when adopting cloud computing services. Government organisations must inevitably accept a degree of risk in many of the aspects of its operations. However, as NIST notes, “many organizations are more comfortable with risk when they have direct control over the processes and equipment involved”, and that with cloud services “some subsystems and subsystem components fall outside of the direct control of a client organization” (2011b, p 21). Cloud computing services are already in use extensively within government (Kamstra, 2013). Therefore, refusing to adopt cloud services cannot be seen as a viable strategy for protecting information risks, as such advice is likely to be seen as out of touch with reality. Therefore the study provides an assessment of the adequacy of governments’ guidance frameworks in preparing government organisations to properly assess the risks, opportunities, and necessary controls for information in a cloud service. In doing so, it indicates direction for future, more rigorous assessments of the effectiveness of information management controls and privacy safeguards implemented by government organisations.

Governments are bound by very strict obligations for managing the privacy and control of data which it collects (Irion, 2012, p 41). It has been asserted that cloud computing “necessarily implies data transfer and, possibly, a trans-border data flow...from this perspective, the legal qualification of the subjects involved with the data flow and the definition of the consequent responsibilities and obligations are fundamental (Djemame et al., 2012, p. 16). I have applied recent public policy research relating to cloud computing to examine the cloud computing strategies and adoption frameworks of six countries: Australia, New Zealand, Canada, United States, Ireland, and the United Kingdom. These countries have significant common heritage in their system of laws and government, and their official use of the English language allows consistent comparison of the guidance. Particular attention was given to the approaches taken by Australia and New Zealand. The research analyses the implications for information management of the various approaches taken by these six countries.

Using the official cloud computing strategy as a starting point (generally, the strategy which was officially endorsed either by the Government Chief Information Officer (CIO), or the responsible Government Minister), the study examined the various guidance documents and processes specifically for adoption of cloud computing which had been published by the studied jurisdictions. The Government CIO or equivalent was selected as the starting point because that function has been given a powerful role within governments, a role which influences and acts as a coordination point for many other traditional leaders in information management.

Literature Review

Definition of cloud computing

The definition of cloud computing used in this study is that put forward by the National Institute of Standards and Technology (NIST), which was used to provide a reference point for cross-jurisdictional comparison. This definition is widely considered to be authoritative (Kesan, Hayes & Bashir, 2013, p 356).

> According to the official NIST definition, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."
>
> The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also lists three "service models" (software, platform and infrastructure), and four "deployment models" (private, community, public and hybrid) that together categorize ways to deliver cloud services." (Brown, 2011)

This study focused specifically on the approach of those jurisdictions to *public cloud* services, which are services “made available to the general public or a large industry group and...owned by an organisation selling cloud services” (NIST, 2011a).

The NIST definition forms part of the cloud computing regulatory framework for the United States government. The definition is also accepted in the cloud computing strategies of the United Kingdom and Ireland. The definition was adopted in the Australian Government’s previous *Cloud Computing Strategic Direction Paper, 2011,* although it is not referred to in the Australian Government’s current *Cloud Computing Policy.* The New Zealand Government has not formally issued a cloud computing strategy, policy, or guidance, but the definition has been used in public presentations by senior officials (Wakefield, 2012). The Canadian Government has not formally issued a cloud computing strategy, policy, or guidance, and so it cannot be established based on publicly available information whether the NIST definition has influenced its approach. So, with the exception of Canada, it can be asserted that the NIST definition has influenced the cloud computing approach of the studied jurisdictions.

Holding close to a definition is important with an emerging technology topic such as cloud computing. Research firm Ovum has noted that "cloud can be easily over-hyped, creating unrealistic expectations and the risk of...a false positive and naive enthusiasm for cloud services" (Hodgkinson, 2012, p 2). This research has focussed on governments' approach to cloud services providers' "enterprise" services, which is to say services for large organisations that are closely integrated with core information technology systems. For example, Amazon Web Services, which was officially launched in 2006, was one of the first major cloud service providers and is cited as a catalyst for the growth of the cloud industry as a whole (Ko, 2012, p 84). Those services which are used peripherally or in niches within organisations are not within the scope of this study. So while cloud computing is provides the underlying platform for social websites such as Facebook, and media services such as Hulu and Netflix (Kesan et al, p 359), the study did not examine policies and guidance for using social media services.

Understanding the information management implications of cloud services

When outsourcing a service, and information, to a cloud service provider, an organisation retains responsibility for the information risks. The implications of this may not be fully appreciated by decision makers. In 2010, a report was conducted for the UK Centre for Protection of National Infrastructure which suggested that there are unresolved "wide-ranging legal or regulatory issues involved in cloud computing including rights to data, security loopholes, outsourcing and subcontracting" (Robinson et al,, 2011, p 26). Cloud providers appear to be no less diligent in their response to security concerns than traditional IT providers. The European Network and Information Security Agency conducted an extensive study in 2009 which found that "the economies of scale and flexibility possible with cloud-based defences permit a robust, scalable and cost effective approach to security but the massive concentrations of resources and data in the cloud present a more attractive target to attackers (Robinson et al., 2011, p 26).

When considering cloud computing services, government organisations are caught between their desire for cost savings and acquiring the latest technology platforms, and their perceived need to maintain firm control over their data. One strong position articulated in response to the perceived threat of cloud services to organisational information is the argument for "data sovereignty". This position has strong adherence from privacy advocates, particularly in the context of adopting offshore public cloud computing (Irion, 2012, p 41). One definition of data sovereignty is "Government's exclusive authority and control over all virtual public assets, which are not in the public domain, irrespective whether they are stored on their own or third parties' facilities and premises" (Irion, 2012, p 41). NIST agrees that negotiating service agreement to address concerns about privacy and security is possible, it notes that the costs of tailoring services in this way "are generally dependent on the degree of deviation from the corresponding non-negotiable, fee-based services" (NIST, 2011b, p 6). NIST explains that this is because such changes can "significantly perturb and negatively affect the economies of scale that a non-negotiable service agreement brings to public cloud computing, a negotiated service agreement is normally less cost effective" (p 8).

Academics have noted the “abstraction of end-user applications from the underlying hardware” is critical to cloud computing (Kushida, Murray & Zysman, 2011, p 2). With control of data location becoming a process managed automatically by software, the physical location of a system’s servers can no longer be used as a means to control risk to an organisation’s data, which may be “may be distributed among multiple physical servers over several states; this may distribute the risk of a single point of failure, but creates multiple possible points for intrusion” (Paquette et al, 2010, p 249). This also means that “data access and distribution may very well be subject to the privacy laws and precepts of the host country (Paquette et, al, 2012, p 249). While the technology architecture of public cloud services could in theory be replicated in a private cloud, “the competitiveness of Cloud Computing service provision critically depends on providers’ ability to build out capacity at a scale far greater than any individual user or firm could afford” (Kushida et al, 2011). While many organisations will focus on applying technological controls to cloud services, it is argued that “the governance and organisational controls applied to the use of these technologies that is the real determinant of the resulting level of maturity in respect of security or privacy” (Robinson et al., 2011, p 39). Robinson also notes that “a highly ‘secure’ technology may be rendered highly insecure by lax security controls and poor governance” (2011, p 39).

The literature uses an analogy with utility providers in the language with which is describes cloud services. Fishenden and Thompson argue that ‘open architecture’ cloud services allow “disaggregation of the ‘black box’ of previously vertically integrated silos, proprietary systems, and opaque-cost structures, enabling easier cost comparison between commoditized components in a manner that resembles, for example, the domestic electricity market” (2013, p 979). Other researchers have noted that “cloud services are uniquely and dynamically configured for the needs of each application and class of users” (Kushida et al, 2011, p 213). Thus, while the economic model has some of the advantages of a utility company, the information management implications of individual deployments of cloud services may be unique.

Concerns have been expressed around both the explicit contractual provision of public cloud services with respect to privacy, and by the management of service outages and failures. Kesan et al have conducted an empirical analysis of the terms of service offered by major cloud service providers’ (2013). They found that “providers take similar approaches to user privacy and were consistently more detailed when describing the user’s obligations to the provider than when describing the provider’s obligations to the user”, and that these terms are essentially of a “non-negotiable nature” (p 341). Providers which have separate privacy policies were found to have “significant advantages being reserved for the service provider, such as the right to amend its privacy policy unilaterally with little notice to its customers” (p 426). The authors conclude that there is a need for a legal framework to assert at a minimum “data mobility and a right of data withdrawal” (p 387). Without these rights, users of cloud services will be unable to effectively respond to changes to services which cause the risks of continued use to exceed an acceptable level.

Public Management and transformation through cloud computing

Public Management, which is the discipline that studies the organisation and management of public sector agencies, provides context to governments’ current approach to the adoption of cloud computing. The extent to which governments are responding to specific regulatory constraints, external political pressures, or inertia and conservatism within government agencies, may be a matter which is best answered by a political scientist. Therefore, this study necessarily assumes that the cloud strategies and policies and their implementation frameworks exist in a straightforward and logical relationship.

The theory and practice of public management have evolved since governments invested heavily in early generations of digital systems, systems which are now obsolete. It has been noted that the United Kingdom has been moving to “a new era of Digital Era Governance” (DEG) since 2000, replacing the previous paradigm of “New Public Management” (NPM) (Fishenden & Thompson, 2013). Darrell West, a director at the Washing D.C. think-tank the Brookings Institute (and former academic and leading scholar of e-government) argues that “there are many success stories from the private sector of better performance through digital technology and organisational change...the question is how best to facilitate innovation in the public sector” (2011, p 17).

Fishenden and Thompson explain that the NPM model promised “competition and incentivization” through the disaggregation of government into corporatised units, but that it instead led to poor results including:

> “increased administrative complexity resulting from the vertical ‘siloing’ of agencies, difficulties in coordinating joined-up service delivery across independent organizations operating within different incentivization structures, instances of service provider fraud, and the ineffectiveness of many large private finance initiatives and outsourcing contracts for a range of reasons that include poor service quality, spiralling cost, and cost-cutting by contractors” (Fishenden & Thompson, 2013, p 978).

Fishenden and Thompson explain that the cloud computing is one of the factors driving the new DEG model for government, which is characterised by “a reaggregation of public services under direct government control around the citizen” (p 978). They argue that the implementation of this model is hampered by the persistence of an “NPM-era commercial model involving unchecked development of monolithic, outsourcing-style private sector involvement in IT-service delivery” (p 982). Instead, it is suggested, that “in contrast to NPM’s focus on disaggregating structures, the Open Architecture approach focuses on disaggregating a continuous process of innovation” (p 996).

In Fishenden and Thompson’s view, developing new systems built on cloud services will be an essential component of the transformation which governments desperately need. To evaluate these claims, it is necessary to look at other scholarship on public management. One major trend in Public Management is wide scale reorganisation of public sectors as a whole, with major changes made in the United Kingdom, Australia and New Zealand in recent years. It has been suggested that the flexibility of cloud services has enabled more flexibility in making changes to organisational structures within government (Margetts & Dunleavy, 2013, p 9). Don Kettl argues that, in New Zealand and Australia, “there is a consensus...that NPM has done a lot of very important work but that it has run its course. People are looking for the next big idea, but there is currently no idea that will galvanise action as the NPM did when it was launched in New Zealand in the late 1980s” (Kettl, 2013, p 43). A “Better Public Services” reform initiative was launched in New Zealand in 2012. In the context of this initiative, Duncan and Chapman warn that it would be easy to put up an “effigy called ‘NPM’” which is “duly burned at the stake, or worshipped, as the case may be”, arguing that it is normal for models of practice to be adapted to “new circumstances and technologies” (Duncan & Chapman, 2013, p 152).

Despite the apparent limitations of the NPM model, there is significant inertia preventing changes to it. Although the NPM model “has rarely delivered the policy outcomes governments have sought,” Fishenden and Thompson allege that “there has been little apparent accountability for such repeated failures, either among officials or among the supplier base”. They go on to argue that “the current NPM-era model, despite its history of failure and cost, thus remains deeply ingrained and embedded” (Fishenden & Thompson, 2013, p 997). In the US, it is noted that “the history of designing, delivering, and managing very large scale federally-developed systems does not offer many success stories to build upon” (Paquette et al, 2010, p 250).

This literature on public management suggests that cloud computing and other innovative technologies are widely seen as having the potential to enable transformation in government, but that governments are yet to successfully fully shift from a public management paradigm characterised by poor technology management and project failures.

Information privacy and technology scepticism

Legal scholars and privacy advocates have been concerned with the information privacy implications of modern computing technologies for some time. Before cloud services became a major segment in enterprise-scale computing market, the information privacy implications of the increasingly powerful internet-based technologies emerged as a significant concern. Popular webcomic xkcd has humorously summarised some of the common opinions on digital privacy (figure 1).

Daniel Solove, a Professor of Law at New York University, has written extensively on privacy in the digital context. He explains that privacy has been traditionally been legally protected by prosecuting “privacy invasions” against specific individuals, but that modern technologies have outpaced the legal concepts. Solove asserts that with the rapid changes in digital information technology, this view “often overlooks the fact that certain privacy problems are structural – they affect not only particular individuals but society as a whole” (2004, p 97). He suggests that “if we look at privacy more as an aspect of social and legal structure, then we begin to see that certain type of privacy harms are systemic and structural in nature, and we need to protect against them differently” (p 97). This increased potential for government to undermine privacy, whether purposefully or not, coincides with a vastly reduced trust in government in the United States: since 1964, trust that the government does the right thing “almost always or most of the time” has reduced from 76% in 1964 to 18% in recent surveys (West, 2011, p 15) Lior Strahilevitz, a legal scholar at the University of Chicago, notes a related concern that there is a distinct lack of appreciation for the value and sensitivity of government-held information: “much of the information in the government’s hands is information that high-level policy makers don’t realize exists, that is poorly organized, and may even be difficult to locate”. He suggests that, by contrast, the commercial incentive to maximise return on all assets which is present in the private sector has driven the development of sophisticated tools and techniques to analyse information assets (2010, p 13).

Solove has argued that the ability of governments to process, store, use and analyse data, rather than the mere ability to collect it through surveillance, is of the greatest concern for privacy scholars.

> [These uses] affect the power relationships between people and the institutions of the modern state. They not only frustrate the individual by creating a sense of helplessness and powerlessness, but also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives. (Solove, 2011)

Solove argues that legal and policy solutions to cloud computing essentially address the concerns about surveillance, and do not adequately address "the Kafkaesque problems, those of information processing. The difficulty is that commentators are trying to conceive of the problems caused by databases in terms of surveillance when, in fact, those problems are different" (Solove, 2011).

The massively increased ability to analyse personal information is not only a result of increased technological capability. It also comes about as a result of cultural and societal changes. It has been stated that increases in government ability to monitor and collect private information "often occur in a time of turbulence or public panic and the state can take advantage of such circumstances to advance other agendas...many of the anti-terrorism and anti-crime measures currently on statute books today are there as the direct result of some major event" (Bannister, 2005, p 74). Solove has studied the emergence of the "digital dossier", by which privately controlled third-party databases collect digital information about individuals. He explains that aggregating a large number of small and individually innocuous details produces information sources which could potentially have major impacts on an individual, including their creditworthiness, their social reputation, and their career prospects (2004, p 21). Tal Zarsky, a legal scholar at the University of Haifa, notes that current data mining techniques, when applied to the vast databases of personal information which have emerged in recent years, "can uncover disturbing behaviour patterns, and assist in ongoing investigation to find criminals and terrorists they are already seeking" (2010, p 82). Zarsky observes that emerging privacy frameworks typically require consent to be granted by an individual for specific uses of disclosed information. He suggests that the status quo when information is collected by governments is that the "citizen might not have conceded to data collection at all...rather, they were forced to provide their data and settle for basic and vague notice of the collection and future uses by governments" (201, p 84).

The positions articulated by legal scholars and privacy advocates outline a perspective focussed on the rights of individuals and the upholding of longstanding legal principles. This is a useful starting point for understanding how governments needs to respond to the privacy implications of using cloud services for storing and managing private information. The services governments are looking to adopt do not necessarily enhance governments' ability to massively aggregate private data, or expose this data to a higher overall risk than it already faces. However, many of the main companies which have attracted concern from advocates for their aggregation of private data, such as Google, Amazon and Microsoft, are also vendors of some of the main cloud services, and this perception among advocates is very important.

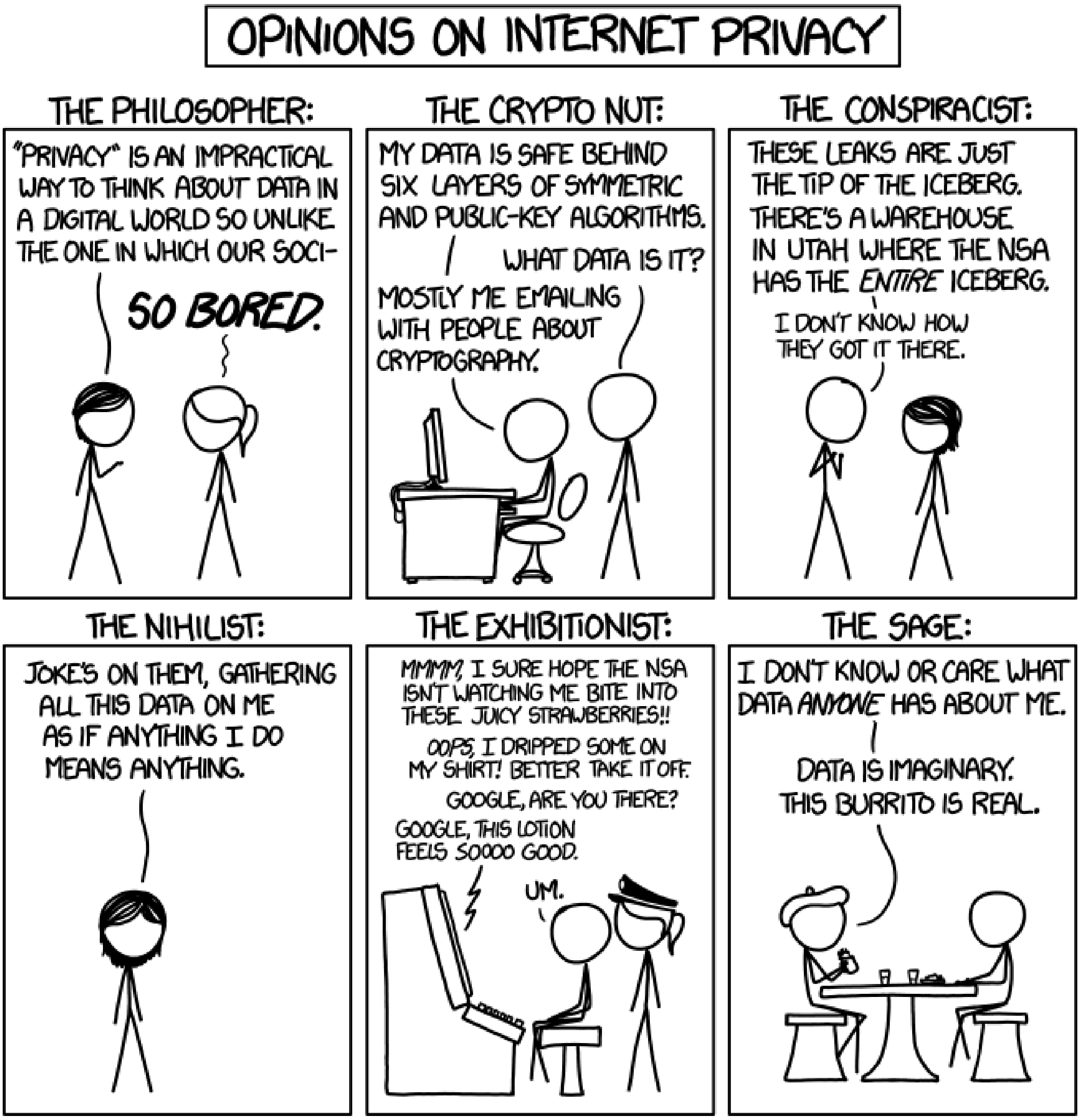
OPINIONS ON INTERNET PRIVACY
THE PHILOSOPHER:
"PRIVACY" IS AN IMPRACTICAL WAY TO THINK ABOUT DATA IN A DIGITAL WORLD SO UNLIKE THE ONE IN WHICH OUR SOCI-
SO BORED.
THE CRYPTO NUT:
MY DATA IS SAFE BEHIND SIX LAYERS OF SYMMETRIC AND PUBLIC-KEY ALGORITHMS.
WHAT DATA IS IT?
MOSTLY ME EMAILING WITH PEOPLE ABOUT CRYPTOGRAPHY.
THE CONSPIRACIST:
THESE LEAKS ARE JUST THE TIP OF THE ICEBERG. THERE'S A WAREHOUSE IN UTAH WHERE THE NSA HAS THE ENTIRE ICEBERG.
I DON'T KNOW HOW THEY GOT IT THERE.
THE NIHILIST:
JOKE'S ON THEM, GATHERING ALL THIS DATA ON ME AS IF ANYTHING I DO MEANS ANYTHING.
THE EXHIBITIONIST:
MMMM, I SURE HOPE THE NSA ISN'T WATCHING ME BITE INTO THESE JUICY STRAWBERRIES!!
OOPS, I DRIPPED SOME ON MY SHIRT! BETTER TAKE IT OFF.
GOOGLE, ARE YOU THERE?
GOOGLE, THIS LOTION FEELS SOOOO GOOD.
UM.
THE SAGE:
I DON'T KNOW OR CARE WHAT DATA ANYONE HAS ABOUT ME.
DATA IS IMAGINARY. THIS BURRITO IS REAL.

Figure 1: "Privacy opinions", from *xkcd, A webcomic of romance, sarcasm, math, and language.* http://xkcd.com/1269/ licensed under a Creative Commons Attribution-Non-commercial 2.5 License

Industry self-regulation and best practice

Cloud computing services providers have in many cases sought to reassure clients that their solutions provide appropriate security and privacy controls. The New Zealand Institute of IT Professionals facilitated the development of the New Zealand Cloud Code on behalf of the New Zealand cloud computing industry. This code is designed so that "professional and responsible cloud service providers benchmark and demonstrate their practices, processes and ethics via an independent third party to build trust with prospective customers" (NZIITP, 2013). In Australia, the Australian Computer Society (with the endorsement from the Federal Government) is leading the development of a consumer cloud protocol aimed at increasing the confidence of small and medium sized organisations in cloud computing (Bajowski, 2013). A simplified version of the NIST definition is used in the New Zealand Cloud Code, with the code requiring that cloud services providers who are signatories to the code "won't say something is 'Cloud Computing; unless it really is" (NZIITP, 2013c).

The Cloud Security Alliance (CSA) is a not-for-profit organisation set up by security researchers and IT security companies with "a mission to promote the use of best practices for providing security assurance within Cloud" (CSA, 2009-13). The CSA maintains a "Cloud Controls Matrix" which defines a standard terminology for security measures (CSA, 2013a). Version 3 of the matrix was introduced in September 2013, after a period of revision which emphasised the need for controls to be auditable (CSA, 2013b). In 2013, the CSA also published an analysis of cloud security incidents, outages and failures which were reported in the media; this analysis was conducted by academics from the University of Waikato and Nanyang University, Singapore (Ko, Lee & Rajan, 2013). Their study found that the cause was not declared for 25% of 172 incidents reported in the period between January 2008 and February 2012 (Ko et al, 2013, p 5). However, the authors noted that there had been improvement in transparency from providers when incidents occurred: "Beginning in 2010, cloud providers became more transparent with their reports of cloud vulnerability incidents, most likely because Amazon became more open about the causes of their incidents" (Ko et al, p 7).

Increasing the openness of the industry in this way will be helpful for providing organisations, and the general public with confidence in cloud computing. However, given the very specific requirements for government cloud computing, these initiatives will not alone support the considerations necessary for government adoption of cloud computing.

Research questions

The key research question was:

1) *How have the governments of the selected nations prepared for the information management implications of implementing cloud computing systems within government?*

The following subsidiary research questions were also been developed:

2) *What are the restrictions being put in place on public sector organisations storing data with cloud computing providers?*

3) *What type of public sector data is being permitted to be stored with cloud computing providers?*

4) *How are public sector organisations directed to implement mechanisms to retain control of the data?*

5) *How are public sector organisations directed to meet existing accountability requirements?*

6) *How do these differ across the jurisdictions, and in particular how closely aligned with the other jurisdictions is New Zealand?*

Different jurisdictions may adopt different approaches to allowing government data offshore for a variety of reasons (Robinson, 2011, p. 63). For this research project, reasons other than information management implications are not considered for detailed analysis. These reasons may include: overarching legal frameworks and tradition; the cultural importance of privacy; cultural distrust of foreign governments; ideological differences in the fundamental role of government; ideological differences in the role technology can play in government; political expediency; geographical or technological proximity to 'friendly' jurisdictions; sensitivity to cost considerations, and therefore appetite for risks in light of cloud computing's promised cost reductions (Robinson, 2011 ; Mell & Grance, 2009 ; Jansen & Grance 2011). In-depth analysis as to the extent which these factors are influential in particular jurisdictions are likely to be a productive topic for future research; this study's findings into management of information risk may provide a starting point for a more comprehensive analysis.

Research scope

What is driving cloud adoption in the studied jurisdictions?

The adoption of cloud services in government in the studied jurisdictions is apparently driven in part by the public sector's drive to cut costs, as well as its desire to adopt the latest technological innovations . Some researchers consider the shift to cloud computing as an inevitable consequence of progress in information technology, with a recent paper arguing that "it will become increasingly unsustainable for a department to insist on procuring a high-cost, bespoke service that replicates its legacy bureaucracy rather than adapting its bureaucracy to take advantage of a low-cost, standard service" (Fishenden & Thompson, 2013, p 20). Regardless of whether that proves to be the case, there is widespread acknowledged that "the substantial promise of cloud services meets the pronounced interest of many government worldwide, who are conscious of how they spend taxpayer money and who are keen to find ways to do more with less" (Irion, 2012, p 45). This is reflected in the language used in cloud strategies in the studied jurisdictions:

- **the United Kingdom Government** cloud strategy states that "Cloud computing has brought about a step change in the economics and sustainability of [ICT] enabled service provision", and notes that the government's "Digital by Default Agenda puts ICT at the heart of public services". It goes on to assert that "the implementation of cloud computing and on-demand delivery models is central to meeting these challenges" (Cabinet Office, 2011, p 2).
- **the United States Government** cloud strategy states that the "cloud computing model can significantly help agencies grappling with the need to provide highly reliable, innovative services quickly despite resource constraints" (Kundra, 2011, p 1).
- **the Australian Government** Cloud Policy states a goal of being "a leader in the use of cloud services to achieve greater efficiency, generate greater value from ICT investment, deliver better services and support a more flexible workforce" (AGIMO, 2013, p 5).
- **the New Zealand Government** ICT Strategy predicts that a "services-based model, and a maturing of the risk assurance framework" combined with "digital self-service channels" for citizens and "unlock[ing] the full economic potential of the government's information holdings", together with "other improvement programmes", will "deliver the required savings and necessary enhancements in service delivery" (Dept. Internal Affairs, 2013, p 6).
- **the Irish Cloud Computing Strategy** "[acknowledges that cloud] has the potential to fundamentally change the nature of ICT delivery over time, and to provide benefits in terms

of efficiencies, cost effectiveness, speed to market" and a number of other benefits, and consequently "it is anticipated that Cloud Computing will be a key part of the strategic future of ICT in the public service" (Dept. Public Expenditure & Reform, 2012, p 11).

- **the Canadian Government** has not published a Cloud Computing Strategy

The promise of cost savings through technological innovation is not new: a decade ago, there was great excitement at the prospect of e-government, a term which is still extensively used in academia but which is less fashionable in government itself.[1] As one academic noted in 2004, "e-government advocates envision a future in which citizens have 24 hour, 7 days a week interactive access to all important government bureaus" while simultaneously citing as a model the "90% transaction cost savings of the financial industry's implementation of online banking" (Garson, 2004, pp 2-3).

What are the risks in these jurisdictions?

Despite the widely identified opportunity for government to get better value from its ICT spending, and to deliver enhanced services with innovative technologies, there are risks that governments will either fail to capitalise on this opportunity, or risks that governments' implementations of cloud computing will put privacy and information security at an unacceptable risk . It has been noted that "introducing the cloud environment in an organization as vast and complex as the government exacerbates the intricacies and potential risks enormously" (Paquette et al., 2010, p 248). One risk that the study anticipated was that governments would fail to establish realistic guidelines and controls to appropriately manage the risks to information which it puts into a cloud service, with the result that the guidelines either push government organisations to maintain a technology environment which is increasingly difficult to support, or that official guidance is seen to be un-implementable and so cloud services are adopted anyway with no meaningful risk mitigations considered or put in place.

Research paradigm and methodology

This study takes an interpretivist perspective and uses a qualitative methodology. The literature review identified that strategies for information and technology within government are often associated with both political opinions and speculative enthusiasm. An interpretivist perspective allows for these positions to be analysed and contrasted while deemphasizing the need to establish a fixed and concrete interpretation, which would be very difficult for an area which is both speculative and political. As government adoption of cloud is an emerging field, and the frameworks to assess the adoption against are not fixed, qualitative analysis allows more flexibility to analyse the range of approaches across the sample.

[1] The search "e-government" on Google Scholar gives 15,000 results for articles published since 2012.

Data gathering

Method

The study only considered published documents, so if governments have developed strategies, policies and guidance which is only provided internally within public sector organisations, this was not captured in the data gathering phase.

To identify relevant published material, the Government Chief Information Officer or equivalent function for each jurisdiction was identified, and their websites were searched for strategies and policies relating to cloud computing (both manually and with inbuilt site search tools). Research was carried out into the structure of the public sector in the jurisdictions, and other relevant entities were searched for guidance documents relating to cloud computing in the same manner. Functions referenced as having a significant responsibility within documents found by this process were indentified and searched in a similar manner. Google "site:" searches across the .gov.au, .govt.nz, .gov, .gov.uk, .gc.ca, and .gov.ie domain spaces were conducted to ensure identification of relevant documents was not hampered by poor website organisation or faulty site search tools. Finally, all documents were checked for whether they were the most current version.

Challenges

Because this method yielded a small number of relevant documents from New Zealand, and not documents from Canada, broader internet searches were used in an attempt to find further relevant documents. A range of public documents which had not been formally published were indentified in this way.

Because cloud computing is evolving rapidly, the regulatory response is also evolving. In the course of this study, further documents were issued. The New Zealand Government issued a new ICT strategy in July 2013, which contained a strong focus on "as-a-service" ICT. The Australian government "Cloud Computing Strategic Direction Paper" from 2011 was superseded by a new "Cloud Computing Policy" in May 2013, and the Attorney General's Department issued the "Australian Government policy and risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements" in July 2013.

The identified frameworks are referenced in Appendix 1.

Data analysis

The information management guidance and frameworks gathered were narrowed for the analysis phase. The analysis excluded general guidance which was not specific to cloud services (such as detailed information security manuals) and legislation, which were both considered to be out of scope. However, wider documentation was included for consideration in the study of New Zealand, as relating the research findings to the New Zealand context was a key research objective. Documents which were not clearly linked, or weakly linked, to the main strategies and policy were excluded or not closely analysed.

The research questions were used to develop a coding manual. This manual included identifying overall characteristics of the frameworks, and investigating the framework for evidence of specific controls which must be adhered to when adopting a service. The controls which the cloud frameworks were investigated for were drawn from the NIST *Guidelines on Security and Privacy in Public Cloud Computing*, which provides a summary of 20 control recommendations in nine areas: Governance, Compliance, Trust, Architecture, Identity and Access Management, Software Isolation, Data Protection, Availability, and Incident Response (2011b, pp 35-36). Many of these controls were incorporated into the coding manual as they relate to technical ICT security. The NIST guidelines were used as a basis for comparison because they are part of the same suite of publications as the NIST definition of cloud computing, which the study found to have been very influential in each of the studied jurisdictions with the exception of Canada. The coding manual is included in an appendix.

Findings: Managing risks to government information in cloud services

Country summary findings

How have the governments of the selected nations prepared for the information management implications of implementing cloud computing systems within government?

Australia

The most extensive and best coordinated regulatory framework, outside the reference framework of the United States, is provided by Australia. This contains official positions of a number of the core government agencies, while providing a relatively unified and practically useful framework for assessing the information management decisions which must be made when using a cloud service. In doing so, Australia diverges significantly from the approach to adopting cloud computing put forward by the New Zealand Government and the United Kingdom Government.

The Australia Government guidance consists of multiple publications issued by multiple agencies. The core document is the Australian Government Cloud Computing Policy v 2.1 ("the Policy"), issued by the Australian Government Information Management Office (AGIMO) in July 2013. This is supported by the "Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements" ("Policy and Risk Management guidelines"), published in July 2013 by the Attorney-General's Department.

The Policy asserts that the Australian government intends to be "a leader in the use of cloud services to achieve greater efficiency, generate greater value from ICT investment, deliver better services and support a more flexible workforce" (AGIMO, 2013, p 5). The Attorney-General's Department's guidance provides the process to make decisions, based on a risk assessment of the agency's situation and the category of information which would be held in the cloud service.

The Australian framework acknowledges that multiple agencies have a stake in cloud computing policy. The Australian Signals Directorate (ASD) "Cloud Computing Security Considerations" document contains insightful analysis of various information risks of cloud computing, and also describes potential risk mitigations and controls However, these are not described within a process framework which would actually be useable by an organisation looking to make a decision about whether or not to use a service. The utility of the advice which is included is also undermined by a blanket statement that the ASD "recommends against outsourcing information technology services and functions outside of Australia, unless agencies are dealing with data that is all publicly available" (ASD, 2012, p 1). This advice is clearly incompatible with the Policy, which states that "agencies will choose cloud services where the cloud service represents the best value for money and adequate management of risk compared to other available options" (AGIMO, 2013, p 5).

Having multiple regulatory agencies involved in defining and guiding the government's adoption of cloud computing is useful in that it has the potential to bring broad support to that approach. AGIMO, the group lead by the Australia Government CIO, has apparently taken the approach of coordinating multiple agencies' guidance, and publishes or links to these as a single suite of guidance on a web page. However the challenge with so many parties is the potential to provide redundant or even conflicting advice (as in the case of the ASD guidance). The document prepared in conjunction with the Office of the Australian Information Commissioner, “Privacy and Cloud Computing for Australian Government Agencies”, was found not to provide any more substantial advice than that contained in other documents in the suite of guidance, except for some general information about the impact of a yet-to-be implemented amendment to the Privacy Act (p 3). This guide is also positioned as a “non-exhaustive list of issues” (p 1) and therefore does not establish either a set of essential considerations or a logical process for decision making, which vastly reduces its utility.

The guidance of the National Archives of Australia, “A checklist for Records Management and the cloud” which is linked to in the AGIMO suite. While this outlines some important considerations, the checklist of advice largely duplicates that in other documents, and it provides no process by which to weigh the importance of the various considerations it outlines. These various contributing guidance documents reflect wider concerns of misuse and sovereignty risks, and recommend the specification of controls including: agreeing that the information is not disclosed to any subcontractor who is not subject to the same provisions as the main service provider; ensuring that there is a right of discovery across all the service providers systems to identify all information about an individual and correct it if necessary; and strict provisions to ensure the complete deletion of data. With research suggesting that cloud terms of service are “essentially of a “non-negotiable nature”, these guidance documents are unable to help agencies make a call as to whether a particular risk warrants completely discounting a service (Kesan et al., 2011, p 341).

With the publishing of the Attorney General Department’s Policy and Risk management guidelines, Australian government agencies have a clear process to follow to assess risks when considering the adoption of cloud services. This document introduces a requirement for agencies to undertake a risk assessment when adopting cloud services. Where a *public cloud* service will manage an agency’s non-public information, the process requires that the risk assessment is calculated and accepted by an agency head, and where a *public cloud* service will manage personal information, this must also be accepted by the agency’s responsible minister and the Attorney General (p 2).

The effectiveness of this approach can only be established by analysing the impact on specific incidences of cloud service adoption. However, it appears to offer a defined process which would be possible, if challenging to meet. An ongoing challenge for the Australian Government will be managing the multiple guidance documents produced by various regulators, which have the potential to confuse agencies and distract attention from thorough assessment processes. If these documents are not kept up-to-date or rationalised, they are likely to diminish agencies understanding of and enthusiasm for the authoritative process, leading to less effective assessment of information risks and information management impacts by agencies.

New Zealand

As a country which is physically isolated from the rest of the world, New Zealand is also isolated from the major metropolitan centres and their telecommunications and data centre infrastructures. It also has a small population of 4.4 million people. These constraints put the New Zealand government at a significant disadvantage as it seeks to adopt the innovative cloud computing technologies which fundamentally depend on economies of scale and advanced ICT infrastructure. Nonetheless, the New Zealand government has expressed a strong desire to adopt cloud computing.

In August 2012, the New Zealand Cabinet made a decision regarding "Managing the Government's Adoption of Cloud Computing". This decision was released publicly although a number of sections were redacted, including the entirety of the section on "Financial Implications" (p 3). Cabinet acknowledged that "there are significant financial, efficiency, collaboration and innovation benefits to be gained through the coordinated, all-of-government adoption of cloud computing" (CAB Min (12) 29/8A, p 1). The decision also agreed that "an all-of-government 'cloud first' approach be taken for the government's adoption of cloud computing" (p 1).

To implement this decision, it was agreed that the Government CIO "lead work to establish common foundational capability, appropriate policy frameworks and standards, and a service deployment strategy, working collaboratively with relevant agencies and service providers". The Department of Internal Affairs (of which the Government CIO is Chief Executive) was also directed to develop risk and assurance frameworks and guidance, and to "identify and, where appropriate, revise audit and data classification mechanisms", in conjunction with other relevant government agencies (p 2). In the mean time, cabinet "agreed that, until the all-of-government approach is implemented, all State services agencies should obtain guidance from the Department of Internal Affairs before making decisions to adopt cloud-based services " (CAB Min (12) 29/8A, p 5).

These decisions outline a useful framework. However, the guidance and the risk and assurance frameworks, and other documents have not yet been publicly made available and therefore cannot be studied or analysed. Cloud computing guidance published by the State Services Commission in 2009 has not yet been formally discarded, although it is now significantly behind technological developments in cloud computing.

A presentation given to the GOVIS conference 2013 by the Government Cloud Programme Manager, indicates that Software as a Service makes up 82% of the current cloud usage by the New Zealand Government (Kamstra, 2013). Of these services, 52% are hosted offshore (from New Zealand). Statistics about the actual number and value of services, and the type of information used in those services, has not been published. However Software as a Service is noted by NIST as the category of cloud computing where the consumer has the least control over the underlying technology for storage and management information (NIST, 2011a, p 2). This makes a consistent process for understanding and accepting risks particularly important.

In the absence of a definitive policy, the New Zealand position risks losing coordination between the various agencies which have a stake in cloud computing adoption. For example, Archives New Zealand have posted guidance on its website around "What are the Recordkeeping Implications of Cloud Computing?" and the Office of the Privacy Commissioner have published "Cloud Computing – a guide to making the right choices". The flaw of the Archives New Zealand guidance is that it does not provide a process to follow. The Privacy Commissioner's guidance applies to public and private sectors alike. While this guidance could well support aspects of a decision making process, it is unlikely to assist effective decision making by government agencies on its own, and it is not clearly linked to a methodology which can be used by government organisations to weigh, treat and/or accept information risks.

As a whole, this study was not able to ascertain the effectiveness of cross-government strategy to manage the risks and implications of cloud computing for information management.

United Kingdom

The role of providing information assurance of a cloud service is centrally coordinated by the Cabinet Office rather than being conducted by individual agencies. The Cabinet Office has published guidance for cloud service providers to assist in this process, but this guidance is not designed for independent use by agencies. The central process results in services being categorised as appropriate for information with a particular business impact level. Agencies must conduct their own risk assessments on their information to a determined business impact level, and then select services which are assured for that business impact level. The guidance that agencies use for assessing the information's business impact level is detailed, but it is not specific to cloud services. This means that there is not clear guidance available to agencies to conduct their own risk assessments on services and adopt them under their own initiative.

The UK has widely implemented this approach, and there are currently 9000 services offered under the G-Cloud ii and G-Cloud iii contracts. Therefore, it is possible to investigate whether it has had some measure of success. On cost savings and flexibility benefits, the strategy hopes that cloud computing will enable "the move from high-cost customised ICT applications and solutions to low cost, standard, interchangeable services" (HM Government, 2011, p 5). As one scholar notes, it seems the G-Cloud is "effectively trying to play catch-up" for the previous lack of strategic ICT planning (Margetts & Dunleavy, 2013, p 13). On information assurance, the strategy states that "the use of trusted organisations to carry out the appropriate level of assurance in the service on behalf of the rest of the public sector will allow both the suppliers and consumers of services to understand the risks and counter measures" (HM Government, 2011, p 19). The G-Cloud is open about the extent to which it has been used. Between March 2012 and the end of September 2013, suppliers sold £53.55 million of cloud services through the G-Cloud (G-Cloud Sales Information, October 2013). This pales into insignificance when compared to the estimated £17 billion annual IT public sector business (National Audit Office, 2011).

Two conclusions can be drawn from this: either the UK public sector is discouraged by the centralised process of information assurance established by the UK Government Cloud Strategy, and only use cloud services minimally, which would suggest that the strategy is a failure from the perspective of delivering value; or, the UK public sector operates outside the existing regulatory framework for cloud, adopting services independently without the benefit of a comprehensive guidance framework to ensure that information is appropriately managed. This would suggest that the strategy is a failure from the perspective of information assurance and information management.

Like the United States, the United Kingdom has access to a significant domestic market for cloud computing services, especially considering the wider EU. However the approach is not necessarily taking advantage of the opportunity within that market. Overall, this study did not identify a cross-government strategy to manage the risks and implications of cloud computing for information management, and found evidence that the current strategy was a failure.

United States

The United States (US) government does not face the same concerns as the other countries. This is because it has a large domestic market for cloud computing, and therefore many of the attractive services considered offshore by other countries are onshore, within US jurisdiction. The US extensive guidance, which includes policy at a Government CIO level, and guidance issued by NIST provides a reference model for other jurisdictions. In this case, NIST is both a de-facto arbiter of internationally recognised cloud computing definitions, as well as the agency formally tasked by the US government to provide implementation advice. In scoping the design of the research, I was not aware of the extent to which NIST provided the regulatory framework for cloud computing in the US. The US Government CIO's Cloud Strategy does not address the information management aspects of cloud computing in any detail. After briefly listing the necessary considerations of "Statutory compliance, Data characteristics, Privacy and confidentiality, Integrity, Data controls and access policies, and Governance", the strategy refers to online NIST cloud computing resources "for additional discussion and considerations regarding trust and security in the context of cloud computing" (Kundra, 2011, p 14).

Having based the content analysis framework on NIST guidance, using it to analyse itself would be largely redundant. However, the findings of this research did not find any indication that the US government's framework for managing the risks of adopting cloud computing was being shown to be ineffective, and found that it has been highly influential in other countries.

Ireland

The Irish cloud computing strategy acknowledges its concerns about public cloud, and suggests that public cloud is most appropriate for "public-facing and non-sensitive activity" (Irish Government, 2011, p 12). It also acknowledges that its approach, which seeks to develop a "Public Service Community Cloud" within government facilities, "would not benefit from the same economies of scale that cloud providers may achieve in their own environments when operating at a global scale" (p 17). It does provide criteria for public cloud consideration, including "Data Location and Retrieval", "Data protection", "Privacy", "Security Standards" although this is just a list of words or short phrases with no explanation or relationship to an assessment or decision-making process (p 25).

The Irish government is clearly in the early stages of considering its adoption of cloud computing, and the appropriate protections for managing information, but has acknowledged this fact. Consequently, it has limited the scope of types of information which it considers appropriate to put in a cloud computing environment. It has also limited expectations of the benefits. However, it may be that the conservative attitude of the central government is shared in all government agencies, so it is possible that agencies are adopting cloud services without an adequate risk framework to guide them.

Canada

A regulatory framework issued by the Canadian government was not found in a form which would be useful. A paper titled "Cloud Computing and the Canadian Environment" was presented in 2009 by the Chief Technology Officer of Public Works General Services Canada (Cohen, 2009). This paper, or any other paper with apparent official standing, cannot be found on relevant Canadian Government websites, including Public Works General Services Canada (the shared services agency), Treasury Board Secretariat (the host of the Government CIO function), and Library and Archives Canada.

While the study did not find evidence that the Canadian government has a coordinated approach to the cloud, the question remains open as to whether agencies are adopting cloud services without an adequate risk framework to guide them.

Discussion

The research findings suggest that governments' enthusiasm for adopting cloud computing is not matched by their understanding of its implications. Governments have seen the promise of cost savings and innovation from cloud computing, and have stated that it is therefore their intention to adopt cloud computing. While a government may be able to issue a tender for a cloud technology-derived service which has been highly customised to meet its requirements, many innovative cloud services may not be able to respond to such requests (Robinson et al., 2011 p 41). This indicates the need for guidelines which allow a government organisation to assess the risks of a particular cloud service on a case-by-case basis. This assessment should be relative to several critical factors, including the value of its information, and the risks if the information were to be compromised. Crucially, this guidance also needs to provide government organisations with a process to prioritise and make decisions about those identified risks.

The NIST definition of cloud computing was found to have been influential in the documentation produced by New Zealand, Australia, the United Kingdom and Ireland. However, governments have not given sufficient emphasis to the way in which cloud services depend on economies of scale. NIST has noted that "non-negotiable service agreements in which the terms of service are prescribed completely by the cloud provider are generally the norm in public cloud computing" (NIST 2011b, p vii). This is supported by recent quantitative analysis by Kesan et al. (2013, p. 341). Perhaps in acknowledgement of the Australian government's specific circumstances, the NIST definition was not used in its 2013 Policy, having been referenced prominently in the 2011 Strategic Direction Paper.

After analysing their published strategies, polices and guidance for adoption of cloud computing, is was not possible to answer the subsidiary research questions 2-6 across all the countries studied. However, the following broad conclusions can be drawn:

Governments' cloud frameworks are fragmented across multiple agencies, and it is difficult to unify the frameworks

Multiple government functions provide thoughts or opinions on cloud computing. While these functions attempt to coordinate their advice, the matters offered for consideration are typically not contextualised or weighted by importance, which means that they cannot easily inform the process of making a decision. The Australian Government has a suite of up-to-date and well-considered guidance which appears to be closely coordinated between the various regulatory agencies, and even this guidance comes across as fragmented.

Governments rely on generic frameworks and advice for managing information risks in cloud services

This research avoided wading into governments' information security manuals and legislation. However, guidance from the United Kingdom and Australia often deferred to these as sources of the official position when assessing risks, despite the fact that these are non-specific and typically predate the cloud computing era.

Governments' appetites for savings are incompatible with their appetites for risk to information

Driven by the attraction to cost savings, the policies and guidance established by the government of the United Kingdom attempts to assert a process for cloud services which either severely limits the scope of services which could be provided through true cloud computing, by centralising the process to assess and approve cloud services. Alternatively, governments haved specified service requirements which are so divergent from industry norms that they will not match any of the existing cloud services in the market. For example, the New Zealand government's decision (CAB Min (12) 29/8A) to specify that government-wide office productivity cloud services would be provided onshore means that, while the services are technically reproducible, it will not get the benefit of global economies of scale available through services such as Microsoft 365 or Google Docs which are the drivers of cost savings ". This is despite the same decision acknowledging that "an all-of-government 'cloud first' approach be taken for the government's adoption of cloud computing" (p 1).

Another expression of this reluctance may be in these jurisdictions unwillingness to publish any guidance at all. The research methodology assumed that governments would clearly articulate their position of various risks and benefits in order to ensure cloud computing was adopted in a value-adding but risk-managed fashion. Despite publishing a new ICT Strategy in July 2013, the New Zealand government has not yet published further guidance regarding information risks referred to in the most recent public Cabinet Minute (CAB Min (12) 29/8A). The Irish government has not recently released any recent information regarding its ambition for a "Public Service Community Cloud", and the Canadian Government has not issued any information at all. The United Kingdom is continuing with the approach of centrally approving cloud services for its G Cloud.

Conclusions

The study has not been able to make cross-jurisdictional analyses of the cloud guidance frameworks because they simply did not exist publicly in sufficient detail. However, this in itself is an interesting finding. The literature suggests quite clearly that governments will find it inevitable to adopt cloud computing technology as they redevelop and expand their digital services. Government agencies within the studied jurisdictions have their own executive leadership and significant degree of authority to make decisions regarding their organisations investment in information systems. Without clear guidance frameworks, government agencies may independently adopt various cloud services, and the decision-making process around these investment decisions will vary in quality. Given that using cloud services introduce a range of complex issues, including international contract law, privacy, data sovereignty, and fundamentally relate to government agencies existing accountabilities, it is unlikely that these investment decisions will fully align with the risk appetite of government as a whole.

The Australian government provides a framework to guide agencies' leaders to a decision to accept the information risks of a cloud service based on a thorough analysis, and provides extra oversight in situations where personal information is involved. The effectiveness of this approach has not yet been demonstrated; however, it provides a potential basis for consideration in New Zealand and other countries which must adopt offshore public cloud services if they are to enjoy the full benefits of the innovative technologies collectively referred to as cloud computing.

Bibliography

Attorney General's Department, Australia. (2013, July). Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements. Retrieved 30 September 2013, from http://www.protectivesecurity.gov.au/informationsecurity/Documents/PolicyandRiskmanagementguidelinesforthestorageandprocessingofAusGovinfoinoutsourcedoroffshoreICTarrangements.pdf

Australian Signals Directorate. (2012, September). Cloud Computing Security Considerations. Retrieved 30 September, 2013 from http://www.asd.gov.au/infosec/cloudsecurity.htm

Antón, A. I., Earp, J. B., Potts, C., & Alspaugh, T. A. (2001). The role of policy and stakeholder privacy values in requirements engineering. In *Requirements Engineering, 2001. Proceedings. Fifth IEEE International Symposium on* (pp. 138–145). IEEE.

Apperley, I. (2013). Update: Government Cloud New Zealand and Australia. *whatisitwellington*. Retrieved 16 October 2013, from http://whatisitwellington.com/2013/10/15/update-government-cloud-new-zealand-and-australia/

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Stoica, I. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58.

Auffret, J.-P., Estevez, E., Marcovecchio, I., & Janowski, T. (2010). Developing a GCIO system: enabling good government through e-Leadership. In *Proceedings of the 11th Annual International Digital Government Research Conference on Public Administration Online: Challenges and Opportunities* (pp. 82–88). Digital Government Society of North America.

Bajowski, J. (2013, July 16). Canberra backs industry-led Cloud Code. *Government News (Australia)*. Retrieved 12 October 2013, from http://www.governmentnews.com.au/2013/07/16/article/Canberra-backs-industry-led-Cloud-Code/ZDQYQCKATQ

Bannister, F. (2005). The panoptic state: Privacy, surveillance and the balance of risk. *Information Polity*, *10*(1), 65–78.

Bellia, P. L. (2008). The Memory Gap in Surveillance Law. *The University of Chicago Law Review*, *75*(1), 137–179. doi:10.2307/20141903

Bianco, J. S. (2009). Social Networking and Cloud Computing: Precarious Affordances for the 'Prosumer'. *Women's Studies Quarterly*, *37*(1/2), 303–312. doi:10.2307/27655163

Biswell, S. (2013, September). Better Public Services - spotlight on government ICT [online]. *Public Sector*, *36*(3), 16–18.

Brewster, T. (n.d.). Amazon And Google Denied G-Cloud Entry 'As Clouds Not Government Ready'. Tech Week Europe. Retrieved from http://www.techweekeurope.co.uk/news/amazon-google-g-cloud-security-government-100303

Brown, E. (2011, October 25). Final Version of NIST Cloud Computing Definition Published. *NIST Tech Beat*. Retrieved from http://www.nist.gov/itl/csd/cloud-102511.cfm

Buchanan, E. A., & Hvizdak, E. E. (2009). Online Survey Tools: Ethical and Methodological Concerns of Human Research Ethics Committees. *Journal of Empirical Research on Human Research Ethics: An International Journal*, *4*(2), 37–48. doi:10.1525/jer.2009.4.2.37

Cabinet Office, UK Government. (2013). Sales Information - G-CloudG-Cloud. Retrieved 20 October 2013, from http://gcloud.civilservice.gov.uk/about/sales-information/

Center for History and New Media. (n.d.). Zotero Quick Start Guide. Retrieved from http://zotero.org/support/quick_start_guide

Cloud Security Alliance. (2009, 2013). About. Retrieved 12 October 2013, from https://cloudsecurityalliance.org/about/

Cloud Security Alliance. (2013). CSA Releases CCM v3.0 Info Sheet for Updates on New Controls, Domains. Retrieved 12 October 2013, from https://cloudsecurityalliance.org/media/news/csa-releases-ccm-v3-0-info-sheet-for-update-information/

Cohen, R. (2009). Canadian Government Unveils Cloud Computing Strategy & Whitepaper. *ElasticVapor*. Retrieved 14 November 2013, from http://www.elasticvapor.com/2009/10/canadian-government-unveils-cloud.html

Corner, S. (n.d.). Cloud providers urged to collaborate, consider 'country of storage' labelling. Retrieved 12 October 2013, from http://www.smh.com.au/it-pro/cloud/cloud-providers-urged-to-collaborate-consider-country-of-storage-labelling-20130829-hv1hr.html

Crisci, C. L. (2002). All the world is not a stage: Finding a right to privacy in existing and proposed legislation. *NYUJ Legis. & Pub. Pol'y*, *6*, 207.

Crook, J. R. (2010). European Union Approves Interim Agreement Allowing Limited US Access to SWIFT Data. *American Journal of International Law*, *104*(1), 107–111.

Cruz, X. (2013, January). The State of Cloud Computing Around the World: Canada | CloudTimes. Retrieved 13 May 2013, from http://cloudtimes.org/2013/01/28/state-cloud-computing-around-the-world-canada/

CURRY, A. (2011). Rescue of Old Data Offers Lesson for Particle Physicists. *Science*, *331*(6018), 694–695. doi:10.2307/25790275

Danek, J. (2009, October 6). Cloud Computing and the Canadian Environment. Retrieved 13 May 2013, from http://www.scribd.com/doc/20818613/Cloud-Computing-and-the-Canadian-Environment

Davis, S. E. (2008). Electronic Records Planning in 'Collecting' Repositories. *The American Archivist*, *71*(1), 167–189. doi:10.2307/40294498

Department of Finance and Deregulation(July, 2013). Australian Government Cloud Computing Policy. Retrieved 22 September 2013, from http://agict.gov.au/sites/default/files/Australian%20Government%20Cloud%20Computing%20Policy%20Version%202.1.pdf

Department of Finance and Deregulation. (2011a). Cloud Computing Policy and Cloud Computing Strategic Direction. Retrieved 13 May 2013, from http://agimo.gov.au/files/2012/04/2011-001_AGIMO_Circular_Cloud_Computing_Strategic_Direction_Paper.pdf

Department of Finance and Deregulation. (2013). Cloud Computing Strategic Direction Paper. Retrieved 13 May 2013, from http://agimo.gov.au/files/2013/04/final-_cloud_computing_strategy_version_1.1.pdf

Department of Finance and Deregulation. (2012, September). A guide to implementing cloud services. Retrieved 30 September 2013, from http://agict.gov.au/files/2012/09/a-guide-to-implementing-cloud-services.pdf

Department of Finance and Deregulation. (2013, February). Privacy and Cloud Computing for Australian Government Agencies. Retrieved 30 September 2013, from http://agict.gov.au/files/2013/02/privacy-and-cloud-computing-for-australian-government-agencies-v1.1.pdf

Department of Finance and Deregulation, & Australian Government Solicitor. (2013, February). Negotiating the Cloud – Legal Issues in Cloud Computing Agreements. Retrieved 30 September 2013, from http://agict.gov.au/files/2013/02/negotiating-the-cloud-legal-issues-in-cloud-computing-agreements-v1.1.pdf

Department of Internal Affairs (July 2013). New Zealand Government ICT Strategy and Action Plan to 2017. Retrieved 22 September 2013, from http://ict.govt.nz/assets/Uploads/Government-ICT-Strategy-and-Action-Plan-to-2017.pdf

Department of Public Expenditure and Reform. (2012, June). Supporting Public Service Reform. Retrieved 13 May 2013, from http://per.gov.ie/wp-content/uploads/Cloud-Computing-Strategy.pdf

Dertouzos, J. N., Pace, N. M., & Anderson, R. H. (2008). *The Legal and Economic Implications of Electronic Discovery: Options for Future Research* (1st ed.). RAND Corporation. Retrieved from http://www.jstor.org/stable/10.7249/op183icj

Djemame, K., Barnitzke, B., Corrales, M., Kiran, M., Jiang, M., Armstrong, D., … Nwankwo, I. (2013). Legal issues in clouds: towards a risk inventory. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, *371*(1983), 1–17. doi:10.2307/41739965

Duncan, G., & Chapman, J. (2012). Better public services?: Public management and the New Zealand model. *Public Policy*, *7*(2), 151.

ElasticVapor: Canadian Government Unveils Cloud Computing Strategy & Whitepaper. (n.d.). Retrieved from http://www.elasticvapor.com/2009/10/canadian-government-unveils-cloud.html

Fishenden, J., & Thompson, M. (2012). Digital government, open architecture, and innovation: why public sector IT will never be the same again. *Journal of Public Administration Research and Theory*.

Garson, G. D. (2004). The promise of digital government. *Digital government: Principles and best practices*, 2–15.

George, B. C., Lynch, P., & Marsnik, S. J. (2001). US multinational employers: Navigating through the 'safe harbor' principles to comply with the EU Data Privacy Directive. *American Business Law Journal*, *38*(4), 735–783.

Gibson, S. (2010). Digital fingerprints. *Gibson research corporation*. Retrieved from https://www.grc.com/sn/sn-264.txt

Gottschalk, P. (2009). Maturity levels for interoperability in digital government. *Government Information Quarterly*, *26*(1), 75–81.

Gulland, A. (2009). Information commissioner criticises NHS over 'cavalier' treatment of data. *BMJ: British Medical Journal*, *338*(7707), 1350–1351. doi:10.2307/25671703

Gutwirth, S., Leenes, R., De Hert, P., & Poullet, Y. (2012). *European Data Protection: In Good Health?* Springer Netherlands.

Hiden, H., Simon Woodman, Watson, P., & Cala, J. (2013). Developing cloud applications using the e-Science Central platform. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, *371*(1983), 1–12. doi:10.2307/41739966

Hilbert, M., & López, P. (2011). The World's Technological Capacity to Store, Communicate, and Compute Information. *Science*, *332*(6025), 60–65. doi:10.2307/29783972

Hindman, M. (2008). *The Myth of Digital Democracy*. Princeton University Press. Retrieved from http://www.jstor.org/stable/j.ctt7scb3

Hochheiser, H. (2002). The platform for privacy preference as a social protocol: An examination within the US policy context. *ACM Transactions on Internet Technology (TOIT)*, *2*(4), 276–306.

Hodgkinson, S. (2012). *Questions that a chairman of CEO should ask their CIO about cloud services* (No. IT007-000618). London: Ovum.

Hon, W. K., Millard, C., & Walden, I. (2012). UK G-Cloud v1 and the Impact on Cloud Contracts. *Available at SSRN 2038557*.

Ira S. Rubinstein, Ronald D. Lee and Paul M. Schwartz. (n.d.). Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. JSTOR: The University of Chicago Law Review, Vol. 75, No. 1 (Winter, 2008), pp. 261-285. Retrieved 30 May 2013, from http://www.jstor.org/stable/20141908

Irion, K. (2012). Government Cloud Computing and National Data Sovereignty. *Policy & Internet*, *4*(3-4), 40–71.

ISO, E. (2011). IEC 27005: 2011 (EN) Information technology--Security techniques--Information security risk management Switzerland. *ISO/IEC*.

Ives, B., & Jarvenpaa, S. L. (1991). Applications of global information technology: key issues for management. *MIS quarterly*, 33–49.

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. *NIST special publication*, 800–144.

Jones, R. A., & Martinez, J. E. (2012). *Federal Cloud Computing: Strategy and Considerations*. Nova Science Publishers, Incorporated.

Joshi, A., Finin, T., Kagal, L., Parker, J., & Anand Patwardhan. (2008). Security Policies and Trust in Ubiquitous Computing. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, *366*(1881), 3769–3780. doi:10.2307/25197362

Kaleli, C., & Polat, H. (2012). SOM-based recommendations with privacy on multi-party vertically distributed data. *The Journal of the Operational Research Society*, *63*(6), 826–838. doi:10.2307/41508619

Kamstra, L. (2013). An update on the Government Cloud Programme. Presented at the GOVIS 2013, Wellington, New Zealand. Retrieved from http://ict.govt.nz/programmes/government-approach/more-information/

Kashiwagi, Masami et. al. (2013, May 15). What You Must Know About Data Privacy Regulations In Asia Pacific: Be Ready To Comply With Dynamic Regulatory Changes. Forrester Research. Retrieved from http://www.forrester.com/What+You+Must+Know+About+Data+Privacy+Regulations+In+Asia+Pacific/fulltext/-/E-RES95541

Katz, D. S., Allen, G., Cortez, R., Cruz-Neira, C., Gottumukkala, R., Greenwood, Z. D., Whittenburg, S. (2009). Louisiana: A Model for Advancing Regional e-Research through Cyberinfrastructure. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, *367*(1897), 2459–2469. doi:10.2307/40485593

Kennedy, D. (2008). TECHNOLOGY: MASTER YOUR DISASTERS: Make online data storage part of your recovery plan. *ABA Journal*, *94*(9), 34–35. doi:10.2307/27846784

Kettl, D. (2013). 3. Beyond New Public Management: Will governments let citizens and communities determine policy choices and service mixes? In *Putting Citizens First: Engagement in Policy and Service Delivery for the 21st Century* (pp. 39–48). ANU E Press.

Klievink, B., & Janssen, M. (2009). Realizing joined-up government—Dynamic capabilities and stage models for transformation. *Government Information Quarterly*, *26*(2), 275–284.

Ko, R., Lee, S., & Rajan, V. (2012). Understanding cloud failures. *Spectrum, IEEE*, *49*(12), 84–84. doi:10.1109/MSPEC.2012.6361788

Kuada, E., Olesen, H., & Henten, A. (2012). Public policy and regulatory implications for the implementation of Opportunistic Cloud Computing Services for Enterprises. In *Proc. 9th Int'l Workshop on Security in Information Systems* (pp. 3–13).

Kundra, V. (2011). Federal cloud computing strategy.

Kushida, K. E., Murray, J., & Zysman, J. (2011). Diffusing the cloud: Cloud computing and implications for public policy. *Journal of Industry, Competition and Trade*, *11*(3), 209–237.

Lasprogata, G., King, N. J., & Pillay, S. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stan. Tech. L. Rev.*, *2004*, 4–4.

Laszewski, T., & Nauduri, P. (2011). *Migrating to the Cloud: Oracle Client/Server Modernization*. Elsevier Science.

Lee, S. M., Tan, X., & Trimi, S. (2005). Current practices of leading e-government countries. *Communications of the ACM*, *48*(10), 99–104.

Lindquist, E. A. (2013). *Putting Citizens First: Engagement in Policy and Service Delivery for the 21st Century*. ANU Press.

Lindquist, Evert A. (2013). *Putting Citizens First: Engagement in Policy and Service Delivery for the 21st Century*. ANU E Press.

Margetts, H., & Dunleavy, P. (2013). The second wave of digital-era governance: a quasi-paradigm for government on the Web. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, *371*(1987), 1–17. doi:10.2307/23364193

Mell, P., & Grance, T. (2009). Effectively and securely using the cloud computing paradigm. *NIST, Information Technology Lab*.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft). *NIST special publication*, *800*, 145.

Metheny, M. (2012). *Federal Cloud Computing: The Definitive Guide for Cloud Service Providers*. Elsevier Science.

Miceli, C., Miceli, M., Rodriguez-Milla, B., & Jha, S. (2010). Understanding performance of distributed data-intensive applications. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, *368*(1926), 4089–4102. doi:10.2307/25704701

Montoya, S., & Graham, J. D. (2008). *Modernizing the Federal Government: Paying for Performance* (1st ed.). RAND Corporation. Retrieved from http://www.jstor.org/stable/10.7249/op213pv-emr

Nelson, M. R. (2009). Building an Open Cloud. *Science*, *324*(5935), 1656–1657. doi:10.2307/20536490

Nordic Council of Ministers. (2011). *Nordic Public Sector Cloud Computing - a Discussion Paper*. Copenhagen

NZIITP. (2013a). About - Cloud Computing Code of Practice. Retrieved 12 October 2013, from https://www.thecloudcode.org/About

NZIITP. (2013b). Cloudcode - Cloud Computing Code of Practice. Retrieved 21 October 2013, from https://www.thecloudcode.org/Cloudcode

The Cabinet Office (2011). *Implementing the Government ICT strategy: six-month review of progress,* London: The Stationary Officer

Organisation for Economic Cooperation and Development. (2010). *OECD e-Government Studies Denmark: Efficient e-Government for Smarter Public Service Delivery*. OECD Publishing.

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, *27*(3), 245–253.

Pavlichev, A., & Garson, G. D. (2004). *Digital Government: Principles and Best Practices*. Idea Group Pub.

Pearson, S., & Yee, G. (2013). *Privacy and Security for Cloud Computing*. Springer London. Pearson, Siani, & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on* (pp. 693–702). IEEE.

Phythian, M. (2013). The 'Cloud'of Unknowing–What a Government Cloud May and May Not Offer: A Practitioner Perspective. *International Journal of Technoethics (IJT)*, *4*(1), 1–10.

Pigeon, L.-P. (1988). *Drafting and Interpreting Legislation* (Vol. 44). Carswell.

Poulsen, K. (2013, October 2). Edward Snowden's E-Mail Provider Defied FBI Demands to Turn Over Crypto Keys, Documents Show. *Wired*. Retrieved from http://www.wired.com/threatlevel/2013/10/lavabit_unsealed/

Robinson, N., Valeri, L., Cave, J., Starkey, T., Graux, H., Creese, S., & Hopkins, P. (2011). *The Cloud: Understanding the Security, Privacy and Trust Challenges*. RAND Corporation. Retrieved from http://www.jstor.org/stable/10.7249/tr933ec

ROGERS, D. L. (2011). *The Network Is Your Customer: Five Strategies to Thrive in a Digital Age*. Yale University Press. Retrieved from http://www.jstor.org/stable/j.ctt1nprgc

Rubinstein, I., Lee, R., & Schwartz, P. (2008). Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. *University of Chicago Law Review*, *75*, 261.

Salbu, S. R. (2002). European Union Data Privacy Directive and International Relations, The. *Vand. J. Transnat'l L.*, *35*, 655.

Sarin, L. C. (2012). Siva Vaidhyanathan, The Googlization of Everything (and Why We Should Worry). *The Library Quarterly*, *82*(4), 525–527. doi:10.1086/667446

School of Information Management, Victoria University of Wellington. (2013). Supervision and Preparing your Proposal. Retrieved 6 June 2013, from https://blackboard.vuw.ac.nz/webapps/portal/frameset.jsp?tab_tab_group_id=_3_1&url=%2Fwebapps%2Fblackboard%2Fexecute%2Flauncher%3Ftype%3DCourse%26id%3D_4206_1%26url%3D

Schwartz, P. M. (2009). Preemption and Privacy. *The Yale Law Journal*, 902–947.

Sheridan, J. (2012, November 28). Presentation on Cloud and DCaaS - Australian Institute of Project Managers. Text. Retrieved 20 October 2013, from http://agict.gov.au/blog/2013/01/07/presentation-cloud-and-dcaas-aipm

Snapshot. (n.d.). Retrieved from http://agict.gov.au/blog/2013/01/07/presentation-cloud-and-dcaas-aipm

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age* (Vol. 1). NYU Press.

Solove, D. J. (2011, May 15). Why Privacy Matters Even if You Have 'Nothing to Hide'. *The Chronicle Review - The Chronicle of Higher Education*. Retrieved 13 October 2013, from http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/

Strahilevitz, L. J. (2010). Reunifying Privacy Law. *Cal. L. Rev.*, *98*, 2007.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11.

Supporting Public Service Reform - Cloud-Computing-Strategy.pdf. (n.d.). Retrieved from http://per.gov.ie/wp-content/uploads/Cloud-Computing-Strategy.pdf

Tablan, V., Roberts, I., Cunningham, H., & Bontcheva, K. (2013). GATECloud.net: a platform for large-scale, open-source text processing on the cloud. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, *371*(1983), 1–13. doi:10.2307/41739959

Tambe, P., & Hitt, L. M. (2012). Now IT's Personal: Offshoring and the Shifting Skill Composition of the U.S. Information Technology Workforce. *Management Science*, *58*(4), 678–695. doi:10.2307/41432789

Tonin, M. (2005). Updated employment protection legislation indicators for central and eastern European countries. *Institute for International Economic Studies*.

Turner, M., Jones, M., Poschen, M., Procter, R., Rowley, A., & Schiebeck, T. (2013). Secure data sharing across portals: experiences from OneVRE. *Philosophical Transactions: Mathematical, Physical and Engineering Sciences*, *371*(1983), 1–12. doi:10.2307/41739958

Unknown author. (2010). European Union Approves Interim Agreement Allowing Limited U.S. Access to SWIFT Data. *The American Journal of International Law*, *104*(1), 107–111. doi:10.5305/amerjintelaw.104.1.0107

Vaile, D., Kalinich, K., Fair, P., & Lawrence, A. (2013, July). Data Sovereignty and the Cloud: A Board and Executive Officer's Guide - Technical, legal and risk governance issues around data hosting and jurisdiction. *Cyberspace Law and Policy Centre, UNSW*. Retrieved 19 October 2013, from http://cyberlawcentre.org/data_sovereignty/

Wakefield, S. (2012, April 2). *Cloud Computing - Implications for Digital Preservation Technology.* Presented at the Future Perfect 2012. Retrieved from http://www.slideshare.net/FuturePerfect_/stuart-wakefield-cloud-computing

West, D. M. (2011). *The Next Wave: Using Digital Technology to Further Social and Political Innovation*. Brookings Institution Press. Retrieved from http://www.jstor.org/stable/10.7464/j.ctt1281bm

Zarsky, T. Z. (2012). The Data Mining Balancing Act. In *European Data Protection: In Good Health?* Springer Netherlands.

Appendix 1: Identified frameworks

The data gathering phase identified the following publications for analysis

Attorney General's Department, Australia. (2013, July). Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements. Retrieved 30 September 2013, from http://www.protectivesecurity.gov.au/informationsecurity/Documents/PolicyandRiskmanagementguidelinesforthestorageandprocessingofAusGovinfoinoutsourcedoroffshoreICTarrangements.pdf

Australian Signals Directorate. (2012, September). Cloud Computing Security Considerations. Retrieved 30 September 2013, from http://www.asd.gov.au/infosec/cloudsecurity.htm

Department of Finance and Deregulation(July, 2013). Australian Government Cloud Computing Policy. Retrieved 22 September 2013, from http://agict.gov.au/sites/default/files/Australian%20Government%20Cloud%20Computing%20Policy%20Version%202.1.pdf

Department of Finance and Deregulation. (2011a). Cloud Computing Policy and Cloud Computing Strategic Direction. Retrieved 13 May 2013, from http://agimo.gov.au/files/2012/04/2011-001_AGIMO_Circular_Cloud_Computing_Strategic_Direction_Paper.pdf

Department of Finance and Deregulation. (2013). Cloud Computing Strategic Direction Paper. Retrieved 13 May 2013, from http://agimo.gov.au/files/2013/04/final-_cloud_computing_strategy_version_1.1.pdf

Department of Finance and Deregulation. (2012, September). A guide to implementing cloud services. Retrieved 30 September 2013, from http://agict.gov.au/files/2012/09/a-guide-to-implementing-cloud-services.pdf

Department of Finance and Deregulation. (2013, February). Privacy and Cloud Computing for Australian Government Agencies. Retrieved 30 September 2013, from http://agict.gov.au/files/2013/02/privacy-and-cloud-computing-for-australian-government-agencies-v1.1.pdf

Department of Finance and Deregulation, & Australian Government Solicitor. (2013, February). Negotiating the Cloud – Legal Issues in Cloud Computing Agreements. Retrieved 30 September 2013, from http://agict.gov.au/files/2013/02/negotiating-the-cloud-legal-issues-in-cloud-computing-agreements-v1.1.pdf

Kundra, Vivek. (February 8, 2011). Federal Cloud Computing Strategy. *The White House, United States of America.*Retrieved 13 May 2013, from http://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf

HM Government, United Kingdom. (March, 2011). Government Cloud Strategy. Retrieved 13 May 2013, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85982/government-cloud-strategy_0.pdf

Department of Public Expenditure and Reform, Ireland. (June 2012). Supporting Public Service Reform: Cloud Computing Strategy. Retrieved 13 May 2013, from http://per.gov.ie/wp-content/uploads/Cloud-Computing-Strategy.pdf

New Zealand “Cabinet Minute - Managing Government's Adoption of Cloud Computing CAB Min (12) 29/8A” Retrieved 13 May 2013, from http://ict.govt.nz/library/CabMin12-cloud-computing.pdf

Department of Internal Affairs (July 2013). New Zealand Government ICT Strategy and Action Plan to 2017. Retrieved 22 September 2013, from http://ict.govt.nz/assets/Uploads/Government-ICT-Strategy-and-Action-Plan-to-2017.pdf

Appendix 2: Data coding manual

Identification of variables

Has the jurisdiction adopted the US NIST definition of cloud computing as its working definition? The following are drawn from security and privacy recommendations identified in the NIST Special Publication 800-144 'Guidelines on Security and Privacy in Public Cloud Computing'. Further criteria have been identified and recorded as noted.

Governance

Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services.

Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.

Compliance

Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving:

_ data location

_privacy and security controls

_records management

_electronic discovery requirements.

Review and assess the cloud provider’s offerings with respect to the organizational [legislative and regulatory] requirements to be met and ensure that the contract terms adequately meet the requirements.

_Include provisions in contract with provider to uphold privacy laws and regulations

_Include provisions in contract with provider for data repatriation

_Commercial contracts with providers for data protection and redundancy

Ensure that the cloud provider’s electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.

Trust

Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time.

Establish clear, exclusive ownership rights over data.

_Establish clear obligations specifically for personal data

_Establish clear obligations for classified data

Data Protection

Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to:

_control access to data

_to secure data while at rest, in transit, and in use

_to sanitize data

_compensation for loss or misuse

Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value.

Incident Response

Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident.