FINDING THE SILVER LINING: moving government to the cloud[1]

Introduction

What ever happened to the promise of the paperless office? In 1975, Businessweek[2] confidently predicted that "the use of paper in business for records and correspondence should be declining by 1980 and by 1990, most record-handling will be electronic."

In this modern age of digital marvels – when even the humblest of smartphones is a research library, a news studio, a business centre and a communications hub – we continue to drown in paper. The consumption of paper has grown 400% in the last 40 years[3] and is expected to rise to 440 million tons by 2015[4]. Despite paper being an environmental vandal[5], the paperless office - like the personal jetpack and the hoverboard - has yet to eventuate. However the twin impetuses of cloud computing and the rollout of improvements to broadband may bring us closer to that vision.[6]

In an effort to realise greater efficiencies in the public sector, governments are looking at ICT resources, costs, and benefits and asking whether we can afford to sustain traditional models of ICT infrastructure.

The Queensland Government commenced an audit of its ICT systems in May and it has estimated that it would cost $5 billion dollars over the next three to five years to fix the Government's 50 most vulnerable IT systems.[7] Perhaps predictably, cloud services have been identified as part of the solution to consolidate redundant infrastructure and improve productivity.[8]

The question is not, 'are governments going to move to the cloud?' but, 'when, to what extent, and how will privacy fit within this brave new office?'

It is not the intention of this opinion piece to focus on the privacy risk potential of the cloud—that has been well done on many occasions before.[9] Rather its purpose is to

---

[1] For the purposes of this piece we will simply define 'cloud computing' as the storing, processing and use of data on remotely located servers accessed over the internet.

[2] http://www.businessweek.com/stories/1975-06-30/the-office-of-the-futurebusinessweek-business-news-stock-market-and-financial-advice

[3] http://www.ecology.com/2011/09/10/paper-chase/

[4] http://www.grida.no/graphicslib/detail/paper-and-paperboard-production_13e6

[5] The environmental cost of paper both in production and disposal is significant. See http://papercutz.planetark.org/paper/impact.cfm

[6] See for example - http://theconversation.edu.au/the-nbn-and-cloud-computing-a-marriage-made-in-heaven-4684

[7] *Queensland faces $5 billion IT repair bill* article by John Hilvert in IT News at http://www.itnews.com.au/News/310528,queensland-faces-5-billion-it-repair-bill.aspx

[8] Queensland Government Chief Information Officer and audit leader, Mr Peter Grant, has advocated that governments should rely on cloud providers for email. Ibid.

[9] For example, much of my comment in this piece repeats the excellent points made by Victorian counterpart, Dr Anthony Bendall in '*Forecast: Cloudy but fine?" Privacy risks and potential benefits in the cloud*' 21 March 2012 available at http://www.privacy.vic.gov.au/domino/privacyvic/web2.nsf/files/forecast-cloudy-but-fine-privacy-risks-and-potential-benefits-in-the-cloud/$file/speech_bendall_03_12.pdf.

explore the issue of whether the cloud could actually be privacy enhancing for government[10].

'I come to bury paper, not to praise it.'[11]

There are scatterings of information across the Queensland Government—on over 200,000 work computer hard drives; in in-trays and on desks; in drawers and cabinets; inadvertently left on photocopiers and facsimile machines; saved to a myriad of portable storage devices; and stored on innumerable stand-alone databases.

We've all seen the figures – 90% of the world's data was created in the last two years and every day 18.6 billion[12] GB of data is added to the world's store[13]. Governments are significant creators, users, and repositories of data and the creaking and crackling of paper libraries and innumerable duplicated digital data stores begs the inevitable question: where on earth are we going to put all this information?

The cloud presents as a one-stop storage solution. But modern governments are not monolithic. They are more akin to the building of the Tower of Babel; a conglomeration of stand-alone information silos where the common language which enables the business of government is 'documents'.[14] The flow of information between the administrative organs is the lifeblood of government. And whenever there is mobility of personal information there is corresponding privacy vulnerability.

We have met the [privacy] enemy and they are us[15]

The need for 'hard copy'[16] document flow within government is compounded by its polyglot nature and privacy risk is almost an inevitability of the dissonance of a government's disparate information and ICT systems. A report by Queensland's Auditor-General on information system security in 2011[17] concluded:

> *A whole of government approach that relies on individual agencies to adopt Queensland Government guidance with agency self-assessment is not providing risk management for the protection of Queensland Government information.*[18]

---

[10] As Queensland's *Information Privacy Act 2009* applies only to Queensland government agencies, the discussion in this piece will concern the Queensland State Government only.
[11] Apologies to Mark Anthony in Shakespeare's *Julius Caesar*
[12] A billion = a thousand million.
[13] http://www-01.ibm.com/software/data/bigdata/
[14] In Queensland's *Acts Interpretation Act 1954* document is defined as including:
(a) any paper or other material on which there is writing; and
(b) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for a person qualified to interpret them; and
(c) any disc, tape or other article or any material from which sounds, images, writings or messages are capable of being produced or reproduced (with or without the aid of another article or device).
[15] With acknowledgement and apology to Walt Kelly.
[16] This includes both paper and digital documents.
[17] Auditor-General of Queensland Report to Parliament No. 4 for 2011 *Information systems governance and security.*
[18] Ibid, at page 27.

The Auditor-General went on to remark that while no security incidents had been noted for those agencies previously audited, half of the agencies newly audited had had some form of network security compromise since 2009.

A concomitant question to, 'is the cloud safe?' is, 'is paper safe?' The answer must be no. There are hundreds of thousands of points of entry to government information and most commonly it is people who leave the doors open. A 2011 study[19] found that 32% of privacy breaches involved negligent employees with a further 32% involved business process failures - euphemistically called 'systems glitches'.

A multiplicity of risks versus a single point of failure. It is perhaps just a matter of scale.

'Privacy is [not] a noose around our necks'[20]

There is privacy legislation at the Commonwealth level and in almost every State and Territory in Australia. As privacy practitioners well know, 'privacy concerns' can be equally used to defend not releasing information and vilified as being a barrier to the release of information. In the case of the cloud it is often more demon than angel. The seemingly rigid protections required by privacy and the flexibility of a system where data can literally be located anywhere in the world can appear to be at odds. Certainly, there are many well-reasoned criticisms that privacy laws can prevent the uptake of cloud capacity.[21]

At first glance, Queensland's *Information Privacy Act 2009* (IP Act) appears to be a barrier to off-shore cloud service arrangements. Section 33 of the IP Act sets out the limited circumstances when an agency may transfer personal information outside of Australia; outside of express consent, legislative authority or serious health and safety benefits, the agency must satisfy two out of four requirements[22].
While these provisions may initially appear daunting, a closer examination of the convenient pair of sections 33(d)(i) and (iv) shows that the cloud service vendor is simply required to treat the customer's personal information in a manner consistent with the privacy principles.

---

[19] Ponemon Institute *2011 Cost of Data Breach Study: Australia* March 2012

[20] Unedited comment attributed to Mayor Ron Bellingham, Scenic Rim Regional Council in *Public shouldn't be kept in the dark* article by Jenna Cairney published in the Warwick Daily News 23 October 2010.

[21] See for example -http://www.theaustralian.com.au/business/legal-affairs/pilgrim-warns-of-technical-glitches-in-proposed-overhaul/story-e6frg97x-1226478386265

[22] *(i) the agency reasonably believes that the recipient of the personal information is subject to a law, binding scheme or contract that effectively upholds principles for the fair handling of personal information that are substantially similar to the IPPs or, if the agency is a health agency, the NPPs;*
(ii) the transfer is necessary for the performance of the agency's functions in relation to the individual;
(iii) the transfer is for the benefit of the individual but it is not practicable to seek the agreement of the individual, and if it were practicable to seek the agreement of the individual, the individual would be likely to give the agreement;
(iv) the agency has taken reasonable steps to ensure that the personal information it transfers will not be held, used or disclosed by the recipient of the information in a way that is inconsistent with the IPPs or, if the agency is a health agency, the NPPs.

However, despite there being eleven Information Privacy Principles (IPPs)[23] in Queensland, there are only two principles of significant concern: data security (IPP 4/NPP 4) and disclosure to third parties (IPP11 /NPP 2). Cloud services vendors *should* have little to no involvement in the other areas of operation of privacy law, i.e. collection, access, amendment and secondary use.

'Data security' and 'data sovereignty' are the two single biggest points of contention in discussions about the cloud. [24] Obtaining robust data security and thereby ensuring compliance with the spirit of IPP4/NPP 4 is a no-brainer. Personal information is a subset of the information a government would store in the cloud. While of course governments are responsible custodians of their citizens' personal information datasets, they are also concerned about other highly valuable and sensitive information – Cabinet documents, security and intelligence data, financial information, commercial information and intellectual property. Safeguarding of personal information will automatically fall out of the safeguarding of 'non-personal' government information.

Ensuring data sovereignty - that is, protecting against the bogey of foreign governments accessing Australian data stored in the cloud by through such legislation as the United States' *Patriot Act 2001*, Britain's *Intelligence Services Act 1994,* or even New Zealand's *Security Intelligence Act 1969* - is a frequently cited deterrent to cloud uptake. [25]

However, the 'principles for the fair handling of personal information' provide little protection for data sovereignty. The IP Act provides generous flexibility for 'law enforcement activities' the definition of which is broadly defined and which apply on a national level to any agency or part of an agency, criminal or civil, conducting the activities[26]. Put simply, when it comes down to a government's intelligence services accessing personal information, privacy doffs its cap and respectfully shuffles out of the way.

Twin elephants in the room

Privacy can contribute to the conversation in two related areas: data breach notification and privacy complaints. Data breach notification is not generally[27] mandated for in Australian privacy law (yet) but this does not detract from its undeniable benefits. While the Commonwealth Privacy Commissioner's investigation into the unauthorised access of the personal information of approximately 77 million Sony Playstation customers found no breaches of the Commonwealth's privacy principles, the Commissioner was nonetheless critical of its delay in notifying affected individuals.[28] Playstation allowed seven days to

---

[23] And an equivalent nine National Privacy Principles (NPP)

[24] Op cit at 12.

[25] Hamish Barwick, *Computerworld*, 18 September 2012. *Data sovereignty still misunderstood in Australia*: Microsoft http://www.cio.com.au/article/436682/data_sovereignty_still_misunderstood_australia_microsoft_/ and op cit at 12.

[26] See Schedule 5 of the IP Act and Part II of the Commonwealth *Privacy Act 1988.*

[27] Mandatory data breach notification has just been introduced for e-health records.

[28] http://www.oaic.gov.au/publications/reports/own_motion_sony_sep_2011.html

elapse after discovering the breach before publicising it. The Commissioner noted that the 'delay may have increased the risk of a misuse of the individuals' personal information'[29].

While data is wholly within the control of government – both in terms of location of the data and staff dealings – privacy breach notification can be instigated through other governance mechanisms. Those mechanisms would not be available in the case of a non-government agency. Governments would be prudent to include clear and firm protocols surrounding data breach notification in any service agreement with a cloud vendor.

As in most privacy jurisdictions there is the capacity in Queensland for an individual to lodge a privacy complaint concerning a breach involving their personal information, which can be the subject of a hearing and orders in the Queensland Civil and Administrative Tribunal.

Private sector organisations, domestic or international, are not covered by the IP Act. Although there is the legislative obligation for a contracting government agency to 'take all reasonable steps' to bind a contractor to comply with the IP Act, the obligation does not demand that the contractor in fact be bound.

So who do Mr and Mrs Jones from Gympie in Queensland go to when there has been a breach of their privacy in the cloud and, although the agency had 'taken all reasonable steps' to bind the contractor, the contractor remained unbound? The Jones do not have a contractual relationship with the cloud vendor and it would be impracticable for them to pursue potential civil remedies under international law. In this case the Jones may, through no action or fault on their part, fall into a legal privacy limbo.

While in the Sony Playstation case there was a financial incentive to 'do the right thing' by its customers[30] this may not necessarily be the case for 'customer data' obtained and used by government agencies. However, it is strongly arguable that there is a fiduciary relationship between a government and its citizens which requires that their interests be protected in any dealings the government may have with a cloud vendor.

Summary

This piece does not advocate that governments should move their data to the cloud. Nor does it suggest that the cloud can provide the magic bullet for a government's ICT needs.

There are privacy vulnerabilities associated with the cloud, just as there are privacy vulnerabilities with paper, e-mails, USB keys, smartphones and current ICT models. It may be too late to fully fix the privacy vulnerabilities associated with paper and other physically mobile documents. However, a move to the cloud, with well considered security and accountability safeguards, can not only be compatible with privacy law, it may enhance the protections for all government-held information.

---

[29] Ibid.

[30] While Sony itself did not 'lose' any of its own information, the incident nonetheless cost Sony an estimated $171 million for such remedial actions as the introduction of an identity theft protection program, the 'welcome back to Sony packages', customer support costs, legal costs and reduced profits consequently to the breach.

It may not be hard to find the silver lining in the cloud. We now just need to work on creating a diamond exterior.