Parliamentary information and parliamentary privilege in the age of cloud computing

Mini paper[1]

presented by

David Blunt
Clerks of the Parliaments and
Clerk of the Legislative Council
Parliament of New South Wales

at the 53rd General Meeting of the

Society of Clerks-at-the-Table (SOCATT)

in

Dhaka, Bangladesh

Monday 6 November 2017

[1] The purpose of this mini paper is to elicit discussion and collect information from other jurisdictions. The aim is to then utilise this information in a fuller paper to be delivered jointly with Ms Pauline Painter, of the Department of the Legislative Assembly and an officer from the Information Services Branch in the Department of Parliamentary Services, at the Australian and New Zealand Association of Clerks-at-the-Table (ANZACATT) professional development seminar in Perth, Western Australia in January 2018. Ms Painter, together with her colleagues in the Department of the Legislative Assembly and the Information Services Branch in the Department of Parliamentary Services, has been primarily responsible for the development of the encryption solution to the New South Parliament's current cloud computing issue outlined in the paper. Attached is an Appendix prepared by Ms Painter in relation to the NSW Government's information management framework.

Parliamentary information

Information is the lifeblood of parliament. Without the required information it would be impossible for Members of Parliament to effectively make legislation, hold governments to account and represent their constituents. When they carry out their work Members of Parliament likewise create, share and distribute information. The vast quantities of information come in a variety of forms including but not limited to: pages of Hansard, minutes of proceedings, committee reports, submissions, evidence, annual reports, the reports of parliamentary commissions and independent oversight agencies, tabled documents, answers to questions, correspondence from constituents, hundreds of thousands of emails, social media posts.

As Clerks we are responsible for much of this information: we are in effect the custodians of this information. We are required to lead and manage staff whose job it is to sift, compile, sometimes publish, index and preserve parliamentary information. Effective and accurate record keeping is essential in a parliamentary environment. In Australia recently we have been reminded, through the work of Royal Commissions (eg the royal into the institutional response to child sexual abuse) of the critical importance of proper record keeping and the devastating consequences of poor and inadequate record keeping. Record keeping systems are continually evolving and improving, in part to cope with the vast volume of records but also to ensure records are able to be retrieved in a timely manner. This is particularly important for all of us who rely on precedents and need to be able to locate those precedents under pressure during parliamentary sittings.

Some of the forms of record keeping that were once fashionable are now obsolete (eg microfiche and floppy discs), and electronic records management systems are continually enhanced (eg from TRIM to HPRM8). We are also responsible for the preservation of parliamentary data. (In the case of the Parliament of New South Wales this has led to the establishment of a memorandum of understanding with the State Records and Archives Authority for the transfer of certain records, particularly historic records, into the Authority's care in environmentally controlled purpose built storage facilities, while the Parliament retains the custody and control of the records.)

In an age when there is a constant deluge of information and citizens face information overload, much of which (particularly located on the internet) is of dubious veracity, parliamentary information is uniquely reliable. This very valuable reputational advantage is something that parliaments should jealously protect.

Also critical is the security of parliamentary records and data. This has become increasingly evident over the last two years, with increasing attention being paid to cyber security and threats from a variety of sources. Given the sensitive nature of some parliamentary information, any risk to its security must be carefully managed.

Parliamentary privilege

Parliamentary privilege is those immunities from the general law and those powers recognised at law as reasonably necessary for Parliaments and their members to perform their functions effectively. The most important of these privileges is freedom of speech in debate, but other important privileges include the powers associated with the inquiry function of parliaments and the powers to deal with contempt. In some jurisdictions these privileges are codified in statute, in others they depend on common law doctrines of exclusive cognisance or reasonable necessity, and in many jurisdictions they are found in both statute and common law.

Freedom of speech in debate means that those records and that data that has a close connection with proceedings in parliament is not to be impeached or questioned in the courts or other places out of parliament (places out of parliament being those bodies with powers of legal compulsion and the power to impose legal sanctions). Although there is some contention around the following point, it is asserted by the New South Wales Legislative Council and the Australian Senate that this entails an immunity from not only use, but also seizure, of such information.

The interaction of this immunity with the rule of law and the legitimate work of law enforcement and investigative bodies can sometimes be difficult. In New South Wales this has led to the establishment of memoranda of understanding between the Parliament and the New South Wales Police and the Independent Commission Against Corruption. The Australian Senate and House of Representatives Privileges Committees have, in the last 12 months, conducted inquiries into matters arising from the execution of search warrants by the

Australian Federal Police. The Senate Privileges Committee has since been inquiring into the adequacy of current arrangements for the protection of parliamentary privilege in relation to the work of various law enforcement and investigative bodies when that work touches on the Parliament and its Members and their information.

Not all parliamentary information is sufficiently connected with proceedings in parliament to be immune from seizure, or at least use, in a court or place out of parliament. Members expense records, for example, will in most cases not be covered by parliamentary privilege and therefore not be immune from seizure or use. At least in Australia, Members remain subject to the general criminal and civil law and are not immune from investigation or prosecution and Parliament does not stand in the way of the proper exercise of powers by law enforcement bodies in relation to members' conduct. This point has recently been spelt out by the New South Wales Court of Appeal in a decision dismissing an appeal against conviction from a former Member, Mr Obeid, and is consistent with judicial decisions in other jurisdictions (eg the *Chaytor* decision in the UK.)

And so, to cloud computing…

Cloud computing

Most importantly for the purpose of this paper cloud computing involves the storage of data/files/software on third party servers rather than on one's own servers. More broadly it involves internet-based computing whereby resources, software and information is shared to computers and other devices on demand. In effect resources such as networks, servers, applications, data storage and services are "virtualised" and spread out over the internet rather than being located in a server on the premises of the business owner.

Cloud based computing can be public (ie whereby anyone can purchase cloud based services from a provider) or private (ie where the particular infrastructure is produced for and available exclusively to an organisation). Cloud based computing can take a number of forms:

- it can entail the provision of *infrastructure* (such as a webserver internet link); known as *infrastructure-as-a-service (i-a-a-s)*.
- it can involve a *platform* (whereby a key piece of software is hosted on the provider's infrastructure – eg SAP financial management services and

software are likely to only be available through cloud computing in future); known as *platform-as-a-service (p-a-a-s)*

- or it can take the form of the provision of an application or software package (ie where a specific business application is provided over the internet such as through a portal, and where through using the application the user's data is placed in the hands of the software provider or their data storage provider) known as *software-as-a-service (s-a-a-s)*

The scale of the shift underway globally from on-premises based computing to cloud-based computing is enormous. According to a recent article in The Australian newspaper by Scott Galloway ("A four-way contest with one winner: almighty Amazon," 25/9/2017, pp 17 & 22):

> Today's fastest growing sector in tech is cloud computing. There are several big players in the field, including old and new tech: IBM, Microsoft, Google. The dominant player again is Amazon, with a business launched originally to support its internal computing needs. According to Synergy Research Group, Amazon's cloud offering (called Amazon Web Services) enjoys more than 30 per cent of the market, triple the share of the no 2, Microsoft's Azure, and will register $US16 billion in revenue in 2017.[2]

The benefits of cloud based computing are said to include the following:

- cost savings as organisations can utilize existing services rather than having to develop and host them in-house;
- the opportunity to tap into high calibre and current technologies developed and deployed by cloud-based service providers;
- possibly enhanced security of data storage; and
- enhanced business continuity disaster recovery preparedness.

The risks of cloud based computing include:

- the hosting or storage of sensitive data outside an organisation's own networks, and potentially outside the jurisdiction or even across jurisdictions (in this regard the US 2016 *Microsoft Ireland* case is instructive);
- the centralisation of critical data accessible only via the cloud service provider (which may in fact be an entity the subject of parliamentary inquiry – see for example the recent Australian Senate Committee inquiry into taxation arrangements including multinational tech firms);

- the potential loss of control over access to data held by a cloud service provider; and
- the question of what happens to data if the cloud service provider goes out of business or is taken over.

The experience of the Parliament of New South Wales

To my understanding, up until this point time, the Parliament of New South Wales has only used cloud based computing for two services:

- The hosting of publicly accessible information that is published on the parliament's public website; and
- The storage in the i-cloud of photos, video and music which are stored on the Parliament supported i-devices operated by Members and senior staff.

The issue is of considerable current interest, however, for two reasons.

Firstly, the parliamentary departments are currently working together on the preparation of a long term funding strategy, currently called a "Masterplan." The purpose of this project, and the initial "masterplan" document, the first iteration of which is to be produced before the end of 2017, is to convince the New South Wales Treasury of the importance and relevance of budget bids, as well as being a process for teasing out longer term jointly agreed strategies and priorities. ICT will be one of a number of components of the "masterplan." The development of each component of the "masterplan" has benefitted from the provision of expert consulting advice. The report from the ICT consultants could be reduced to one single strategy: we have been urged to develop a "Cloud Adoption Strategy", which would dovetail with the New South Wales Government's "Digital Government Strategy" and apparently resolve all of the Parliament's ICT needs for the next ten years! Appendix One describes the New South Wales Government's information management framework including its cloud policy.

Secondly, the New South Wales Parliament this year has funding to develop and implement a members' expense claims system that will allow members to lodge expense claims online, including via mobile devices. A number of potential vendors were invited to submit tenders earlier this year. Whilst one bidder outlined an "on-premises" solution, the cloud-based solutions that were proposed were far less expensive. The recommended provider is a small New Zealand company

which provides a solution for the management of travel expenses for corporate travel, so has an obvious relevance and application to the management of the work expenses of members of parliament. Under the proposal the company will host their application and the Parliament's data in the Azure cloud (that is Microsoft) at data centres in Sydney and/or Melbourne.

In order to address the risks associated with the storage of sensitive data about members' expenses in a cloud-based off-site location, the New South Wales Parliament has required an additional level of security. The company providing the solution by default has full administration access to the parliamentary data. A third party encryption solution was purchased with only the Parliament possessing the key to unlock the encrypted data that is stored in the cloud. The solution provider will no longer have access to the raw unencrypted data which will protect Parliament against most of the issues around cloud based solutions (*parliamentary privilege, security issues, no control over staff or vendor policy, using a shared platform with several other organisations etc)*

This additional security will come with a not insignificant additional cost (but with the total cost still considerably less than the on-premises alternative).

Questions for other jurisdictions

The purpose of this brief mini paper is to flag this topic as one requiring attention from Clerks and others with responsibility for parliamentary information. It is hoped to encourage and facilitate discussion amongst colleagues, which will be incorporated into a more detailed paper to be presented, together with colleagues from the Department of the Legislative Assembly and Department of Parliamentary Services in January 2018. The following are some of the questions on which the views of colleagues across the Commonwealth would be greatly appreciated:

- To what extent are parliaments already using cloud computing, including for the storage of parliamentary information?

- What sort of communication has taken place with members and other stakeholders about the use of cloud computing, including for the storage of parliamentary information?

- Are there some categories of parliamentary information which are so sensitive that they must continue to be stored on-premises? If so, what are some of those categories?

- How are other public sector bodies addressing the risks associated with the use of cloud computing and to what extent can their learnings be applied to the parliamentary context?

- What specific safeguards should be put in place to protect parliamentary privilege in relation the use of and access to parliamentary information when it is stored in the cloud or in off-premises cloud based data storage centres?

- How important is it that any parliamentary information stored in the cloud or a cloud based data centre be physically located within the same jurisdiction of the parliament in question? Is this even possible to guarantee?

- Given the importance of contractual arrangements with cloud computing providers, would there be benefit in parliaments sharing their experience and expert advice as they negotiate with the providers?

Appendix prepared by Ms Pauline Painter, Department of the Legislative Assembly.

NSW Government Information Management Framework

The NSW Government Information Management Framework helps agencies manage data and information. It includes laws, policies, standards and implementation tools. It includes the ICT Strategy, which was originally launched in 2012 and updated in 2015; with the Digital + 2015 Strategy added the same year.

The NSW Government ICT Strategy and Digital+ 2015 Final Update set out the Government's plan to:

> …build capability across the NSW public sector to deliver better, more customer-focused services that are available anywhere, anytime; and to derive increased value from the Government's annual investment in ICT[3].

Cloud Policy

Another element of the framework is a NSW Government Cloud Policy, issued in August 2015. It states that NSW Government agencies:

> …will evaluate cloud-based services when undertaking all ICT procurements. The decision on the appropriate ICT delivery model will be based on an assessment of the business case, including the cost benefit analysis and achieving value for money over the life of the investment.
>
> The positive experience of NSW agencies so far with the benefits of cloud services leads to the expectation that ICT procurements for commoditisable, non-core business solutions will be provided via cloud-based services – unless there is a specific consideration preventing this from happening. These services would ordinarily be procured from the ICT Services Catalogue or the GovDC Marketplace. [4]

The plan aims to promote openness, mobility and uptake of cloud platforms. The framework represents a paradigm shift from previous NSW government practices, which relied on onsite data centres and will lead to the dispersal of agency data to third party vendors, other state and federal government agencies, non-government

---

[3] https://www.finance.nsw.gov.au/ict/sites/default/files/resources/MigrationServicesandCloudReadinessAssessmentServicesStandard.pdf

[4] https://www.finance.nsw.gov.au/ict/resources/nsw-government-cloud-policy

agencies and various research institutions. Whilst this shift offers significant opportunities for government, it also creates new risks.

Risk management

To adapt to the new ICT environment, Government agencies have developed ways to identify whether external service providers are capable of providing adequate levels of confidentiality, integrity and availability of service. They have developed new ways to ensure that their expectations and legal requirements can be met. Agencies have also had to develop new techniques to maintain control over their data once they relinquish direct line of control.

Research conducted with a number of NSW Government agencies[5] shows that there is no one single approach to managing sensitive data. This is mainly due to the varying capabilities of Cloud service providers. Each service providers is evaluated against the project requirements and deliverables.

The approach taken by an agency is primarily risk based. Agencies must comply with Information Security Policy mandatory requirements[6]; however they are able to customise the process to fit their objectives. The controls defined an agency can be tailored to account for the service providers vulnerabilities. For example, the same piece of data may require that vendor 1 encrypts the data set whilst vendor 2 does not have the same requirement. This could be because vendor 1 has a particular vulnerability which does not exist in vendor 2, as vendor 2 has identified additional assurances and controls.

Case Study: Department of Family and Community Services – External Party Risk Assessment Framework

The Department of Family and Community Services have developed an External Party Risk Assessment Framework[7], which is provided to other departments on request. This guideline assesses the security of external parties that an agency intends to share information with or to which it plans to outsource services. The Framework outlines a standardised approach to ensure agencies meet the requirements of the following:

[5] Family and Community Services; Department of Finance, Services and Innovation; Department of Justice; Office of State Revenue and Office of Director of Public Prosecutions
[6] https://www.finance.nsw.gov.au/ict/priorities/managing-information-better-services/information-security
[7] Fedele-Sirotich, Matthew, FACS, 2014, External Party Risk Assessment Framework

- Privacy and Personal Information Protection Act 1998
- NSW Government Cloud policy
- NSW Digital Information Security policy
- NSW Government information classification and labelling guidelines
- Health Records and Information Privacy Act 2002[8]

It provides a risk-based framework for assessing information security practices, as well as numerous resources which can be used during the entire lifecycle of an external party engagement. These include a:

- sharing risk profile matrix based on the data classification/risk (data impact) and the external party
- contractual agreement for information sharing
- security questionnaire and security Request for Tender questionnaire.

Conclusion

Evidence collected from the agencies showed that there is no single solution to the management of sensitive data in the Cloud, with agencies taking a risk based approach, taking care to evaluate all the options that are presented to them by service providers. Agencies seem content with working with multiple service providers and having data located in various locations. For them, the controls were the key element, not the location of the data.

[8] Fedele-Sirotich, Matthew, FACS, 2014, External Party Risk Assessment Framework, p. 3