Parliamentary information and the challenges (and opportunities) of technology

Paper presented jointly by

David Blunt[1], Pauline Painter[2] and Neil Dammeral[3] [4]

Parliament of New South Wales

Australian and New Zealand Association of Clerks-at-the-Table (ANZACATT) professional development seminar

Perth, Western Australia

25 January 2018

Precis: This paper begins with a discussion of the nature of parliamentary information. It then deals with changes in the way in which information is accessed, and changes in the systems and support available to manage parliamentary information. A key theme is cloud computing, its application, adoption and implications for parliaments. There is a brief discussion around capital and recurrent funding and a brief description of the organisational transformational implications of moving to an "as-a-service" model of ICT support. The paper then discusses the critically important issue of cyber security. Whilst most of the paper draws heavily on the New South Wales experience, two UK case studies are highlighted in relation to cyber security. The paper concludes with a brief discussion about parliamentary privilege and its implications in this area, before posing a number of questions for discussion.

[1] Clerk of the Parliaments and Clerk of the Legislative Council.

[2] Knowledge and Information Manager, Department of the Legislative Assembly.

[3] Senior Manager IT Services, Department of Parliamentary Services.

[4] The authors would also like to acknowledge the invaluable assistance provided (including in relation to an earlier version of part of this paper delivered in November 2017) by Louise Hanna, Operations Manager IT Services, Department of Parliamentary Services.

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. In addition to that uniquely "parliamentary" information, parliaments also run enterprise resource planning information systems which hold significant HR, financial and project management data. Members also hold large volumes of information including correspondence from constituents, hundreds of thousands of emails and social media posts.

As Clerks-at-the-Table we are responsible for much of this information: we are in effect the custodians of this information. We are required to sift, compile, publish, index and preserve parliamentary information. Effective and accurate record keeping is essential in a parliamentary environment. In Australia we have recently 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 potentially 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. It has also led to the digitisation of important historical records of proceedings.)

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

Changes in the way in which information is accessed

Being connected via the internet is now essential and is something that we all take for granted. We all rely on our smartphones for connectivity and many of us conduct our day to day business via our phones, for example, banking, buying clothes, household goods, ordering groceries and paying our bills. We also stay connected to work, checking and responding to emails, long after normal office hours. Australians are embracing the internet for business and personal use more than ever before:

- In the second half of 2016, the volume of data downloaded through broadband connections was 23 percent greater than the first half of the year, continuing the long term trend of growing internet usage.
- In June 2016, 94 percent of adult Australians used the internet to conduct banking, pay bills, or buy/or sell goods and services.[5]

Increasingly Members of Parliament, colleagues and members of the public and other stakeholders expect (not unreasonably) to be able to access parliamentary information using the internet and smart phones or other similar devices. They also expect transactions with the parliamentary administration to be seamless and efficient.

Changes in the systems and support available to manage parliamentary information

The Parliament of New South Wales is a large provincial parliament. There are 135 Members across the two Houses, the annual budget is around $160 M and there are 597 employees including Members' staff. A Parliamentary Information Technology Section was established in the late 1980s and personal computers were rolled out to Members and staff in the early 1990's. Over time the PITS grew in size to employ approximately 18 staff and contractors. Servers were established on site, located in an on-premises server room, with all network support undertaken in-house. Whilst some business systems have been purchased off-the-shelf, other business systems have been developed in-house. It is only in recent years that more business system development and change projects have been outsourced and contract managed.

In 2012 the New South Wales Government adopted a fundamentally new approach to the use of ICT based on the idea of ICT being made available 'as a service', rather than the traditional approach of buying hardware and software. This was enshrined in the NSW Government's ICT Strategy.

[5] Australian Federal Government, *Australia's Cyber Security Strategy, Enabling innovation, growth and prosperity*, First annual update 2017, p.8

This reflects a trend in public and private enterprises to migrate from on premise ICT to the delivery of ICT 'as-a-service' (a-a-S) from offsite in public, private or hybrid clouds. Given the requisite funding, the Parliament of NSW is about to begin to move towards the implementation of just such a model. Key to as-a-service models is cloud computing.

Cloud computing

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 are 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 delivery involves the delivery of on-demand shared computing resources (everything from applications to data centres) globally over the internet on a pay-for-use basis.[6]

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:

> 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, and Google. The dominant player again is Amazon, with a business launched originally to support its internal computing needs. According to Synergy

[6] Louise Hanna, Operations Manager, NSW Parliament IT Services Department, Department of Parliamentary Services

> 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. [7]

Evidence shows that in the private sector, the use of cloud technology is on the rise, as businesses are becoming increasingly aware of the multiple benefits cloud computing can have in terms of efficiency and profitability. Whether it's private, public, hybrid or a mix of various cloud computing models, the technology is now used by at least 70 percent of U.S. organisations, according to IDG Enterprise's 2016 Cloud Computing Executive summary.[8] For the 2015-16 year, the Australian Bureau of Statistics (ABS)[9] said that the move to cloud technologies by Australian businesses had jumped to 31 percent (survey had a sample size of 6750 businesses). The use of paid-for cloud products grows with the company's headcount; adoption is at 25 percent for businesses with 0-4 employees, and 60 percent for companies with a 200+ headcount.

The most cited factor for not adopting a cloud service remains insufficient knowledge, the ABS reported. It is mostly businesses in the agriculture, forestry, and fishing industries that aren't as comfortable with cloud computing. However, companies in the heavily regulated finance sector also commonly said they were worried about the risk of a security breach should they go down the cloud path.

But almost two thirds of all businesses said there were no factors limiting their use of the technology. The ABS noted the media and telecommunication industries were the most fervent adopters of predominantly software-based cloud services. Gartner said Australia's cloud market would reach A$6.5 billion, up 15 percent from last year, thanks predominantly to a boom in software-as-a-service adoption. Worldwide Gartner said the market would jump by 18 percent to reach US$246.8 billion.[10]

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.

[7] Scott Galloway, "A four-way contest with one winner: almighty Amazon," *The Australian*, 25/9/2017, pp 17 & 22

[8] Forbes, *13 Biggest Challenges When Moving Your Business to the Cloud*, https://www.forbes.com/sites/forbestechcouncil/2017/06/05/13-biggest-challenges-when-moving-your-business-to-the-cloud/#84bca899b0ec, accessed 13/1/18

[9] http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/8129.0Main+Features12015-16?OpenDocument

[10] https://www.itnews.com.au/news/cloud-computing-adoption-in-australia-is-booming-468833 accessed 15/1/18

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;
- 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 chief benefits listed by organizations that have successfully moved to the cloud include increased efficiency, ease of access, simpler administration and management, and overall lower costs.[11]

Australian Parliaments and the cloud

For Parliaments, particularly in Australia the take up has been much slower. The following is a simple summary of cloud adoption in state and federal Parliaments (it does not include individual applications).

Name of Parliament	Cloud adoption Yes/No
Commonwealth	Yes
Australian Capital Territory	Yes
Victoria	Yes – hold encryption key
South Australia	Yes – outsourced (No DPS)
New South Wales	Limited
Western Australia	No
Tasmania	No
Queensland	No
Northern Territory	No

Table 1: Summary of Cloud Adoption in Australian Parliaments

Additionally, anecdotal evidence in NSW suggests that Members are increasingly making use of cloud based applications such as drop box and google drive, independent of parliament supported systems.

Until recently, the Parliament of New South Wales has only used cloud based computing for three services:

[11] Forbes, *13 Biggest Challenges When Moving Your Business to the Cloud*, https://www.forbes.com/sites/forbestechcouncil/2017/06/05/13-biggest-challenges-when-moving-your-business-to-the-cloud/#84bca899b0ec, accessed 13/1/18

- The hosting of publicly accessible information that is published on the parliament's public website;
- The Parliamentary Library system; 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.

Last year the New South Wales Parliament received 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.

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

NSW Government agencies and the cloud

This is a similar picture to the wider NSW Government where NSW agencies have an expectation that ICT procurement 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.[12] Research conducted with a number of NSW Government agencies[13] showed that there is no one single approach to the management of cloud implementation. This is mainly due to the varying capabilities of Cloud service providers, to provide the specialised project requirements and deliverables and the appetite

[12] https://www.finance.nsw.gov.au/ict/resources/nsw-government-cloud-policy accessed 15/1/18

[13] Family and Community Services; Department of Finance, Services and Innovation; Department of Justice; Office of State Revenue and Office of Director of Public Prosecutions

of Chief Executives and Chief Information Officers to want to move to the Cloud. Agencies such as NSW Fire and Rescue have lead the way and demonstrated the benefits of cloud adoption.

When asked about how they managed their sensitive data, the approach taken by the agencies was primarily risk based. Agencies must comply with Information Security Policy mandatory requirements[14]; however they are able to customise the process to fit their objectives. The controls defined by 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.

For some public sector agencies the reasons for taking a cautious approach to migrating to cloud computing go beyond security issues. Just as important are issues around control over systems and processes (particularly for agencies that have a track record of successfully developing sophisticated, customised information systems and software), and the responsiveness of service providers, particularly when things go wrong. Of course, these are the same sorts of issues that need to be addressed in relation to any outsourced service.

Capital and recurrent funding

In a public sector context acquisition and the on-going asset management (replacement) of on-premise information systems is largely financed by capital funding. The ongoing management and administration of these assets is financed through the use of recurrent funds. The move to off-premise ICT as-a-service has some interesting implications for this funding model.

Capital funding at the level required both to fund new initiatives and manage existing asset replacement schedules is not guaranteed. For many public sector organisations, the development and upgrade of information systems becomes a sporadically timed and ad hoc upgrade pattern that is subject to the availability of funding rather than a strategically planned approach. Whilst capital funding is not guaranteed, recurrent funding always seems to be reducing in real terms, which has implications for maintenance of existing information system assets. Further, the growth in use, by software vendors in particular, of a subscription based model to generate revenue has also put increasing pressure on recurrent funds.

[14] https://www.finance.nsw.gov.au/ict/priorities/managing-information-better-services/information-security accessed 10/1/15

A move to off-premise ICT as-a-service will reduce the need for capital funding for asset replacement. However, it will require the provision of sufficient levels of recurrent funding to ensure appropriate services can continue to be purchased and contracts managed.

Organisational transformation

For the parliament of NSW the transitional arrangements for the migration to a cloud or hybrid cloud/on premise solution is expected to be undertaken over a 3 year period and incorporate the following components:

- Development of a Cloud Strategy – this strategy would look at all data repositories maintained by Parliament and consider the most appropriate strategy on a case by case basis. It would also consider the impact of issues such as Parliamentary Privilege.
- Development of a new Vendor/Contract Management Model
- Undertake Review of Enterprise Resource Planning Requirements
- Undertake a Go to Market Exercise for a New ERP Platform
- Commence the implementation of fundamental changes to the existing financial model
- Implement cloud strategy – requiring a migrations of existing on premise information architecture to a state that aligns with the agreed cloud strategy

While this 3 year program is underway, it is necessary to maintain the existing asset replacement program without making fundamental changes to the underlying information architecture – for this reason funding for hardware asset replacement, on-going ERP systems and the continuing enhancement of Parliamentary information systems will need to be continued.

Cybersecurity

One of the major considerations when moving systems to the cloud is security. Having information and data located off site potentially increases the risks, or at the very least changes them from those experienced when the information is located on premise. Additional security such as encryption keys and multi factor authentication may need to be considered.

Words such as cybersecurity, cybercrime and cyberattack now form part of our everyday vocabulary, even though ‘cyber’ was only added to the Oxford English Dictionary in the 1980s.[15] Unfortunately, what comes with being online is the increase risk of being a target for cybercrime or being hacked. The cybersecurity environment is constantly changing and evolving and at a strategic level governments are struggling to keep up with threats as

[15] http://www.oed.com/ accessed 14/1/18

technology rapidly advances.[16] For example, Meltdown and Spectre are the names of two serious security flaws that have been found recently within computer processors. They could allow hackers to steal sensitive data without users knowing, one of them affecting chips made as far back as 1995.[17] Cloud services are also affected; Google said it updated its cloud services, but that customer action may be needed for some of its Cloud Platform systems. Amazon said all but a 'small single-digit percentage' of its Amazon Web Services EC2 systems were already protected, but that 'customers must also patch their instance operating systems' to be fully protected.[18]

So what is cybersecurity? In simple terms it involves the protection of computer systems connected to the internet. Figures vary, but according to Australia's Cyber Security Strategy 2016, cybercrime is estimated to cost Australians over $1 billion each year.[19]

2016 and 2017 sharpened our awareness to the world of cyberattacks. The hack and release of information from the US Democratic National Committee by Russian cyber actors in the lead up to the 2016 US Presidential election demonstrated how targeted disclosures of stolen information can interfere with processes underpinning Western democracy.[20] Many Australians remember the night of the e-Census when overnight cybercrime eroded the trust in the government to deliver on an assurance of the protection of our personal data, with the hashtag #Censusfail trending globally.[21]

To help with attacks the Federal Government has established the Computer Emergency Response Team (CERT) Australia who have reported 10,351 incidents, of which 363 were more serious incidents affecting systems of national interest.[22] These attacks include Spear Phishing, which are emails containing a malicious link or file attachment. This remains a popular exploitation technique with methods used becoming more convincing and difficult to spot. Hackers target personnel in order to gain access to corporate networks; individuals with access to large amounts of personal or corporate information online make it easy for adversaries to target individuals or their organisation. The techniques are becoming more sophisticated with hackers using personal and professional information and their social

[16] Nicole Brangwin, *National Security – cybersecurity,* Australian Parliamentary Library Research Publications, accessed 12/12/2017, https://www.aph.gov.au/About_Parliament/Palriamentary_Departments/Parliamentary_Library/pubs/Briefingbook45p/Cybersecurity

[17] https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-computer-processor-intel-security-flaws-explainer accessed 14/1/18

[18] https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw?CMP=Share_AndroidApp_Gmail accessed 15/1/18

[19] Australian Federal Government, *Australia's Cyber Security Strategy 2016*, p.15

[20] Australian Federal Government, *Australia's Cyber Security Strategy, Enabling innovation, growth and prosperity*, First annual update 2017, p.9

[21] Australian Federal Government, *Australia's Cyber Security Strategy, Enabling innovation, growth and prosperity*, First annual update 2017, p.10.

[22] Australian Federal Government, *Australia's Cyber Security Strategy, Enabling innovation, growth and prosperity*, First annual update 2017, p.10

networks. In this way, targets of spear phishing emails are duped into opening malicious attachments and links. More recently we have seen incidents of ransomware reported in the media, these campaigns are constantly evolving and highly successful, with almost all delivered by email. They target a broad range of sectors, including government, resources, business, educational institutions and home users. Ransomware encrypts files on the computer and then directs the victim to a webpage with instructions on how to pay a ransom in bitcoin to unlock the files. The ransom emails often contain a threat of further fines or fees to pressure the recipient into taking action and the ransom typically doubles after 24 hours if not paid. In some cases files are progressively deleted until the ransom is paid. The most famous ransomware attack happened in May 2017 when the global WannaCry attack hit over 300,000 computers, affected over 200,000 people through 45,000 attacks in 99 countries. It famously affected the UK's National Health Service putting people's lives at risk. The main problem was that patches provided by Microsoft to fix this problem had not been installed leaving organisations vulnerable to attack.[23]

> Notable events in 2016 and 2017 expanded Australian's awareness of how cyber security can impact on our lives. Public expectations for improved privacy, integrity and availability of online services will only increase. Government will need to be better at anticipating and responding to future cyber security challenges to prevent shocks.[24]

Case Study – Cyber Attack of UK Houses of Parliament and Scottish Parliament

A case study within a parliamentary context was the attacks in 2017 on the UK Houses of Parliament and the Scottish Parliament. The UK Houses of Parliaments have 9,000 users with 50,000 connected devices. The protection and security of these devices is maintained by the Parliamentary Digital Service and a dedicated cyber team of 10 people, managed by Steven Mark, the Director Cyber Security Programme and based in a new Security Operations Centre. A Digital Strategy has been implemented which contains a three year cyber security programme. The programme was put to the test in May 2017 when it survived the WannaCry ransomware attack; however on Friday 23 June 2017 both Houses of the UK Parliament sustained a 'determined cyber-attack by hackers attempting to gain access to MPs' and their staffers' email accounts'.[25] The hackers were attempting to find weak passwords in order to gain access to emails. The attack continued for 24 hours, looking continuously for different entry points. In a blog put out by the parliament, Rob Grieg, the founding Director of the Parliamentary Digital Service, commented on 30 June 2017:

[23] The Guardian Newspapers online, accessed 14/01/18, https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs

[24] Australian Federal Government, *Australia's Cyber Security Strategy, Enabling innovation, growth and prosperity*, First annual update 2017, p.10

[25] https://www.theguardian.com/politics/2017/jun/24/cyber-attack-parliament-email-access 12 December 2017, accessed 14/1/18

> 'This went on for several hours as the attackers hit the network from servers all over the world. Towards the end of the attack our systems blocked 48,000 attempts to get into the network in a single hour.'[26]

In order to prevent this, the Parliamentary digital services team gave priority to the core systems of the Parliament and kept them up and running to ensure democratic activity could continue. Changes were made to remote accounts to block the hackers however this resulted in staff not being able to access their emails on phones and tablets outside of the Westminster precinct. The Guardian reported that a House of Commons spokesperson advised that the lack of remote access was not part of the attack but a result to protection measures dealing with the incident. 'Parliament has disabled remote access to protect the network'.[27] Accounts were compromised in the early part of the attack and some email data was taken, although less than 1 percent of accounts were affected. No systems on the Parliamentary precinct were affected.[28] Members of Parliament tweeted and spoke about the attack, including the Leader of the Opposition, Mr Jeremy Corbyn, speaking at the Glastonbury Festival. He commented:

> 'I think this indicates just how vulnerable we are to cyber-attacks and our cyber–security. We have to be investing in cyber-protection – it is a huge issue. We all rely on computers, we all rely on emails, and we all rely on digital records. You wouldn't leave your building without importing documents under lock and key. The computer is just the same.'[29]

Lessons learned from the Westminster attack led to several improvements in the security of the Scottish Parliament environment including increasing password length and complexity for user accounts. The technical changes on password policy were put in place before the end of June, meaning that future changes to passwords would have to take account of the new complexity and password length rules. In addition to increasing password security, plans were put in place to introduce multi factor authentication on the email environment post summer recess.

On the 19 August 2007, an as yet unknown third party launched a 'brute force' attack, attempting to guess the passwords for multiple Parliament accounts. The attack was very similar to the attack on the UK Parliament at Westminster and was a sustained and determined attack on many of the Scottish Parliament email accounts. The attack locked

[26] https://pds.blog.parliament.uk/2017/06/30/responding-to-the-cyber-security-incident-in-parliament/ accessed 8/1/18

[27] https://www.theguardian.com/politics/2017/jun/24/cyber-attack-parliament-email-access 12 December 2017, accessed 14/1/18

[28] https://pds.blog.parliament.uk/2017/06/30/responding-to-the-cyber-security-incident-in-parliament/ accessed 8/1/18

[29] https://www.theguardian.com/politics/2017/jun/24/cyber-attack-parliament-email-access accessed 15/1/18

out multiple network accounts which in turn disrupted the normal working practices of the staff and Members affected.

The attack was declared a major incident and managed via the well-established incident management processes. The Parliament was in recess and the main service impact was a short period (approximately three days) where email services was not available from smartphones and tablets. Significant effort was expended over a sustained period (approximately 2 weeks) from the IT function, the National Cyber Security Centre, and key suppliers to investigate, remediate and provide the required assurance that no accounts had been compromised.

The attack has been recorded as a crime by Police Scotland Cyber Crime Unit and the National Cyber Security Centre have shared the intelligence gathered through the attack with other security agencies in order to try an identify the perpetrator. A cyber awareness campaign for all users was already in place, but the attack was used as an opportunity to emphasise the importance of good password and other security practices.[30]

Has the horse bolted?

The challenge for NSW is to ensure that future cloud security policies are not about 'closing the stable door after the horse has bolted'. It must always be proactive not reactive, and try and stay one step ahead of the hackers and keep pace with the ever changing environment. Online security can be easily compromised and people can become complacent, which presents a new set of threats; cyber security is everyone's responsibility. This vigilance needs to continue in contract negotiations with cloud vendors, patches and upgrades must be installed immediately and vendors must be able to act in the best interests of the Parliament at all times. Tim Maliyil, of AlertBoot, who sits on Forbes Technology Council comments:

> 'Will the cloud be more secure than my internal data centre? Can my cloud provider maintain my uptime standards? Will their technical support address my problems quickly? The answer is a resounding "Yes!" to all of these questions when dealing with a mainstream cloud provider in 2017. I had the same fears in 2010 when I migrated to the cloud. I also reduced my hosting expenses by 75 percent by migrating our systems to a cloud provider'.[31]

[30] Alan Balharrie, Head of IT, and Ken Hughes, Assistant Chief Executive Scottish Parliament

[31] Forbes, *13 Biggest Challenges When Moving Your Business to the Cloud*, https://www.forbes.com/sites/forbestechcouncil/2017/06/05/13-biggest-challenges-when-moving-your-business-to-the-cloud/#84bca899b0ec, accessed 13/1/18

Parliamentary privilege

Parliamentary privilege is the immunities from the general law and the 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. Where law enforcement and investigative agencies overstep the mark and seize privileged material entire Houses of Parliament become fully engaged, with concern crossing party lines. This was evident in relation to the Breen matter in NSW,[32] and NBN / Conroy matter in the Australian Parliament.[33] This is because of the potential chilling effect of the seizure of such material on the flow of information from citizens and stakeholders to Members which information assists Members perform their roles of making laws and holding the executive government to account.

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

[32] NSW Legislative Council, Privileges Committee, *Parliamentary privilege and seizure of documents by ICAC*, December 2003, and *Parliamentary privilege and seizure of documents by ICAC (No 2)*, March 2004.

[33] Senate Standing Committee of Privileges, *Status of material seized under warrant*, 163rd report, December 2016, and *Search warrants and the Senate*, 164th report, March 2017; and House of Representatives Privileges and Members' Interests Committee, *Claim of parliamentary privilege by a Member in relation to material seized under a search warrant*, November 2016.

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.)

For many members the information which is held by some parliaments (eg NSW) which might be regarded as most sensitive from members' perspective will not in fact be privileged information. Hence the lengths the Parliament of NSW has gone to in applying an additional level of encryption and security to the members' entitlements information which is to be processed via the new portal and stored in an off-premise cloud. Parliamentary information includes significant amounts of personal information provided to members by constituents. Members are rightly very protective of this information. Schemes for the reporting of data breaches under, for example, the National Data Beaches Scheme raise challenging issues for parliaments, as for other organisations which hold personal information.

On the other hand, much of the parliamentary information which is clearly privileged (eg parliamentary business papers, answers to questions, committee reports) is exactly the sort of information that parliaments are seeking to make more accessible in an effort to engage better with citizens. In the case of the Parliament of NSW this information, which is published on the Parliament's website, is already stored/held in the cloud.

It is difficult to be definitive about the precise categories of information that are clearly privileged and also of acute sensitivity, as these are really only explored and identified on a case-by-case basis (and, for example, under the NSW and Federal MOUs with investigative and law enforcement bodies referred to above, through a process in which privilege is claimed by a Member). However, we would tentatively suggest that the following are two of the sorts of categories of information that will be of acute sensitivity and for which, under an ICT as-a-Service model, arrangements will either need to be made to retain the information on-premise or to have further additional security layers implemented in contracts with cloud providers:

- Submissions received but not made public by committees and transcripts of in camera hearings; and
- Information provided to and retained by Members for use in parliamentary proceedings including but not limited to information provided by whistle-blowers.

The first of these categories of information is easily identified and no doubt business systems will be able to be implemented to enable the management of this information as required by parliamentary officers. The second category of information is far more complex as it is likely to be diffuse and managed by, in the case of the Parliament of NSW, up to 135 members and their staff. Having in place business systems and record management policies and procedures, and ensuring they are consistently applied, to ensure the appropriate management of this information will be a challenge.

Questions for discussion

The following are posed as questions for discussion:

- 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?