Submission No 16

INQUIRY INTO CYBERSECURITY

Name: Dr Bruce Baer Arnold

Date Received: 21 September 2020

Portfolio Committee 1 – Premier and Finance
Legislative Council
Parliament of New South Wales
6 Macquarie Street
Sydney NSW 2600
law@parliament.nsw.gov.au

17 September 2020

Inquiry into Cybersecurity

This submission responds to the Committee's invitation to contribute to its inquiry regarding on cybersecurity and digital information management in New South Wales.

The submission reflects my teaching of law at the University of Canberra. I have doctoral and other qualifications relevant to the Committee's inquiry, alongside acknowledgment in a range of reports by law reform commissions, parliamentary committees, human rights and regulatory bodies.

The submission does not represent what would be reasonably construed as a conflict of interest.

Dr Bruce Baer Arnold
Asst Professor, Law
University of Canberra

cybersecurity and digital information management in New South Wales

(a) The number of cybersecurity incidents and data breaches involving NSW Government agencies

Experience in Australia and elsewhere over the past twenty years demonstrates two matters of concern that are relevant to the Committee's inquiry.

The first is that incidents, in particular large-scale ongoing exposure of sensitive data, are often not immediately identified and thus not addressed. We have for example seen systemic problems at the Australian National University (unauthorised access over several years by state-aligned overseas actors) and at the national parliament. There has been unauthorised disclosure of medicare data and refugee data held by the Commonwealth government. There has been exposure of data held by the University of Sydney, breach of transport data and the recent exposure of data about some 250,000 people regarding their interaction with the NSW government. Overseas some breaches have lasted for years and involved sensitive health, credit, relationships and other personal data alongside illicit access to technical or other data that does not relate to individuals and thus is not addressed under enactments such the *Privacy Act 1998* (Cth) or the *Health Records & Information Privacy Act 2002* (NSW). Many of those incidents are readily foreseeable and preventable. They are also currently inadequately addressed under Australian and overseas law.

In considering the number of cybersecurity incidents involving NSW government agencies several comments are pertinent.

<u>Differentiate number, severity and frequency</u>

In building resilience in data handling as a foundation of public administration and strengthening community perceptions of the effectiveness of government agencies (and thence the legitimacy of Government) it is necessary to look beyond raw counts of the number of incidents. On a strategic basis the Government should recognise that some incidents are trivial: they do not result in a substantive harm to individuals or an agency's reputation and do not pose question questions about an agency's ongoing performance. Some incidents however have the potential to result in serious injury to one or more people, to affect many people, foster public distrust and disrupt core public administration functions. Some cybersecurity incidents are isolated and properly addressed. If they are frequent the number tells us that there are problems with corporate governance, information architecture, training and learning.

My suggestion is accordingly that the Committee contextualise 'numbers'.

<u>Known unknowns</u>

The history of cybersecurity incidents in Australia and overseas is a matter of what might be characterised as the 'known unknowns'. The community sees some reports about incidents, sometimes because the media have prompted public/private sector entities to respond to a breach or other problem. Specialists may have a stronger sense of severity and incidence, often because they study data management and have informal contacts within government, business and academia. Data managers within organisations should have a sense of what is happening within their organisation or their field (for example health services).

I refer to 'unknowns' because we collectively do not have a comprehensive picture of incidents. That is unsurprising, for several reasons. One – the most worrying – is that some organisations did not identify that a breach had taken place (and in some instances was ongoing) as distinct from a disruption to service. Many entities do not publicly report incidents, particularly on a timely basis. There is scepticism among data management professionals about the sharing of bad news.

One conclusion is therefore that 'numbers' are indicative rather than definitive. In retrospect we know that some breaches have occurred but were not detected and addressed at the time. There are 'unknowns' and figures presented to the Committee on an open or confidential basis may not be representative.

Another conclusion is that there is a need for comprehensive consolidated reporting to the NSW Parliament on an annual basis of the number and nature of incidents regarding 1) state agencies and 2) non-state agencies that provide services on behalf of the state. That reporting should cover incidents *per se* and thus not be restricted to personal information, in other words extend beyond privacy.

Emphasise learning

In a piece several years ago I commented that incidents are as likely as death and taxes. In thinking about best practice we should look beyond raw numbers and instead evaluate what has happened and what might happen, particularly what might cause significant harm. Many incidents are attributable to not learning, one reason why the preceding paragraphs are pertinent. That learning involves designing and implementing better architectures on the basis of what has gone wrong in the past. It also involves greater attention to systemic approaches that address concerns regarding over-reliance on service providers, system releases that are determined by the electoral cycle and design that under the umbrella of a whole-of-government digital strategy involves patching legacy systems.

(b) The monitoring and response to cybersecurity incidents and data breaches across the NSW Government

There is disagreement within the data management sector regarding best practice in monitoring and responding to incidents, including data breaches. One concern has been the notion of data breach fatigue, in other words a fear that consumers and other stakeholders will be so discouraged by recurrent news of incidents that breaches will become normative, consumers will become fatalistic and managers organisations will assume negligent practice is acceptable on the basis that 'everyone does it'. Given preceding comments a more positive approach is desirable and achievable. Stakeholders should be seeing a coherent whole-of-government approach to security incidents in which the community can see that government is 1) acknowledging the existence of incidents and 2) reporting evaluations of the significance of incidents and 3) being seen to learn from those incidents on a proactive basis, in other words ensuring that the same problems do not occur in different ministries/agencies.

That approach requires

- Appropriate resourcing (including technical expertise) within agency and whole of government audit units
- Identification and prioritisation regarding incident detection, response, learning and disclosure in agency data management plans
- A stronger commitment to effective privacy by design as a basis for improved efficiency
- Disclosure in agency annual reports, with an emphasis on evaluation rather than merely formalistic reporting of the number of incidents
- A data management ethic within agencies and within service providers to those agencies that emphasises their role as data custodians – gathering, holding.,

processing and disseminating data on behalf of the community – rather than weakly-accountable data owners.

(c) The policies and procedures underpinning the management of digital information by the NSW Government

Governments gain attention by releasing Artificial Intelligence strategy documents and Digital Transformation strategies that are often driven by the need to be seen to be doing something with a digital flavour but do not adequately address issues such as privacy protection and effective oversight by governance watchdogs such as the Commonwealth's Australian National Audit Office. IT trainwrecks such as RoboDebt, CensusFail and the national identity hub are unsurprising but avertable. Governments more broadly have been emphasising whole-of-government or broader cyber security strategies, which in practice are a tacit acknowledgement that ministerial over-reach and institutional resistance have prevented achievement of much broader visions of coherent cross-agency data management under a 'cyber czar' or an entity such as the Commonwealth's Digital Transformation Agency.

In considering the policies and procedures underpinning the management of digital information several issues are relevant in stepping beyond such grand plans.

1) Data custodianship – it is traditional for managers in the public and private sectors to construe their function as a matter of data ownership rather than custodianship. A shift to custodianship will serve to minimise concerns regarding privacy (see below) and foster the legitimacy of public administration in an environment where there is increasing distrust of government.

   Custodianship is particularly relevant given initiatives such as the Commonwealth's large-scale data sharing plan under the auspices of the Office of the National Data Commissioner and proposed *Data Availability and Transparency Act*, involving sharing between Commonwealth agencies (and eventually state/territory agencies) and private sector bodies (research and otherwise) of data collected on a mandatory basis.

2) Outsourcing – the withering of capacity within government has been exacerbated by often ill-considered of data management services to the private sector and more broadly the outsourcing of government services to not-for-profit/for-profit welfare, health and other services providers. Outsourcing per se is not inherently antithetical to good government (ie in terms of accountability, cost and value for money). However there remain concerns regarding inadequate design in service acquisition and supervision.

   There also remain concerns regarding cybersecurity vulnerabilities on the part of service providers who perform functions for government, hold sensitive personal data but have inadequate cybersecurity. One example is the recent ransomware incident involving Anglicare. In essence, if the NSW government and its peers are relying on the private sector for service provision there must be a requirement that those providers are cyber capable and there must be resourcing within government to verify that capability on an ongoing basis rather than merely at the point of initial outsourcing. That verification has a cost; the cost is an acceptable matter of good governance and addresses perceptions that governments are 'paying a buck to pass the buck' to another entity.

3) Looking ahead to IoT – I referred above to the enthusiasm among Governments for artificial intelligence, both because AI has the smell of modernity and because it is perceived as an opportunity to fix intractable problems with administrative systems that cannot be easily changed alongside reducing human resource costs. Experience with RoboDebt suggests caution. The Committee may however consider the need for addressing emerging cyber security vulnerabilities with the Internet of Things, for example in school and health networks. Popular anxieties about a cybergeddon in which the sewage system stops working and planes drop from the sky are misplaced but there is a need for a forward-

looking view that anticipates vulnerability in for example hospitals and that builds robustness into the state's rail network.

(d) Systems management within NSW Government agencies including outages, backups and cyber security;

See above

(e) The financial costs and other impacts of cybersecurity incidents, data breaches and outages involving NSW Government agencies;

There hasn't been a comprehensive public study of the financial costs of incidents (including data breaches and outages) at the government level anywhere in Australia (ie not for the Commonwealth or state/territory governments). Overseas there have been studies of some egregious incidents such as exposure of data about millions of veterans in the United States. Identification of the cost to business and agencies of service disruption is achievable. Identifying direct costs of data breaches is more challenging; indirect costs such as expenditure on system redesign are identifiable if sought.

There are two costs beyond the financial, both of which are relevant for government. The first is reputational harm: can you trust the agency that was blithely indifferent to cybersecurity (eg through inadequate system design/maintenance and supervision of staff) and should you accordingly 'vote' for the Minister? The second is the cost to individuals who are the subject of a data breach, whether through large-scale exposure of data covering many people or realisation that an official (for example a police officer) has been misusing privileged access on a personal basis. In law there is a fundamental problem because it is rarely possible to definitively link the cost of identity crime to a specific breach.

(f) Expenditure on cybersecurity, digital services and digital infrastructure across the NSW Government;

Disquietingly, there is no coherent picture of expenditure on cybersecurity, digital services and digital infrastructure across the NSW government. The absence of consolidated data and of evaluation is concerning. Provision of that picture as a basis for public evaluation should be prioritised and is achievable through for example standard reporting protocols on an agency by agency basis. It should include data on outsourcing of data management services, something that will foster both accountability and competition. The latter is important given perceptions in the IT services sector that government is a generous and often quite forgiving milch cow.

(g) The management of public access to digital information under GIPA and similar processes including coverage of mobile based and online platforms;

See above

(h) Contractual arrangements between the NSW Government and providers of digital services and infrastructure, including:

(i) Provisions relating to cybersecurity generally; and

(ii) Reporting obligations and the monitoring of cybersecurity incidents;

See above.

(i) The extent and impact of outsourcing of government information systems, including:

(i) Outsourcing to entities which are owned overseas;

(ii) The risks involved with outsourcing government information systems

See above.

(j) The support provided by the NSW Government to local councils and other organisations in relation to cybersecurity

See above

(k) The NSW Government's response to cybercrime in the community generally

A salient assessment is that the government needs to be realistic about its responsibilities and opportunities regarding cybercrime, for three reasons. The first is that it does not have sole responsibility: it needs to work with the Commonwealth, in conjunction with the other jurisdictions and with business. The second is that cybercrime is a portmanteau term, covering a range of offences (not all of which involve an illicit financial benefit). The third is that NSW, along with other governments, should avoid the temptation to 'fix' cybercrime by passing new enactments. In practice a more effective response is to build capability within government, both within agencies and within the NSW Police. The latter involves training, recruitment and reward (for example to address perceptions common in law enforcement agencies that 'real' and thus 'serious' crime is exclusively a matter of physical violence addressed by 'feet on the street' rather than fingers on a keyboard.

(l) Any other related matter

The Committee's terms of reference include consideration of data breaches. As noted above some breaches are restricted to commercial and technical information. Others involve personal data that might include contact details (the recent avoidable NSW breach covering some 200,000 people) and might include health, financial or other data. We often construe data breaches as a matter of identity crime aimed at providing the offender with a wrongful financial benefit. It is important however to recognise that many data breaches are an invasion of privacy, a disregard of the individual's legitimate freedom from arbitrary interference. In making sense of cybersecurity as a matter of respecting privacy it is pertinent to note several considerations.

The NSW Government has recently led the other Australian jurisdictions in a reform of defamation law. That reform involves cooperation in dealing with an intractable area of law. There is scope for the Government to encourage a coherent national privacy regime that incorporates recommendations by a succession of law reform bodies, including parliamentary committees and the Australian Law Reform Commission that have called for a statutory cause of action (aka the privacy tort) to address serious invasions of privacy by public/private sector entities. Such a reform would address the egregious inconsistency in statutory asnd non-statutory protection across Australia. It would also realign the expectations of officials and service providers regarding responsibilities. It would not impermissibly inhibit media activity, preclude law enforcement or otherwise erode the constitutionally implied freedom of political communication.

A corollary, something immediately achievable, is reinforcement of a cyber ready culture in the public sector by appropriate funding of an independent information commissioner.

Australian experience is that underfed watchdogs lack institutional capacity, are wary of biting that hand that feeds them, are not respected by the entities they notionally supervise and experience disengagement by the public.

In dealing with cybersecurity the Government needs to set an example to the private sector by walking its own talk. Minister Victor Dominello in introducing the *Road Transport And Other Legislation Amendment (Digital Driver Licences And Photo Cards) Bill 2018* (NSW) told Parliament

> I do not think there is any debate in this Chamber when it comes to putting the privacy of the citizen front and centre. Indeed, when we drafted the Data Analytics Centre legislation—the Data Sharing (Government Sector) Act 2015, as it was appropriately titled—we made sure that the Privacy Commissioner was involved from the ground up in the steering committee so that we achieved the right outcome. In preparing this legislation, we engaged the Privacy Commissioner because privacy is beyond politics. It is an absolutely enshrined right of the citizen.

In practice the engagement of the Privacy Commissioner in design and supervision of government digital initiatives has been weak, late and ineffective. If privacy is indeed beyond politics there must be a greater emphasis on

1) meaningful privacy impact assessments and

2) privacy by design from the first stages of digital initiatives rather than something treated as a tick box requirement once the system architecture is in place.

Irrespective of the problematical nature of the claim to have 'absolutely enshrined' privacy as a right, the exposure of Service NSW information about some 186,000 people – indicates that privacy is not put 'front and centre' by the Government and by what appears to be a service provider. The Minister is reported as stating that shifting to "true end-to-end digital services" will make it "more difficult for criminals" to replicate the Service NSW incident. I have commented on the need for a forward-looking approach rather than preparing to fight yesterday's battles, given that the 'end-to-end' services will introduce new security risks that need to be identified and addressed prospectively rather than retrospectively.

Disclosure

In addressing privacy breaches there is a need for timely disclosure. In the Service NSW incident that needed to be quicker than four months and without the Minister's obfuscation that the affected people were receiving "hypercare", a term that does not have a legal meaning and in practice appears to be little more than a marketing statement worthy of condemnation by the Committee. Citizens respect governments who step up in acknowledging problems rather than engaging in the sort of egregious denial evident in the Commonwealth's response to RoboDebt.

Assistance

In construing governments as data custodians the citizens should have legal remedies for harms and governments should facilitate solutions, for example by paying for credit watch services for all individuals placed at risk through the avoidable data breach. Such assistance is becoming standard practice regarding private sector breaches. It is a mechanism for citizen self-help rather than a solution; as such it is an acceptable cost of public administration.

Reporting

Further, the NSW Government and its peers should engage in timely and full disclosure through a public report on an independent investigation of what went wrong and what has been learnt on a systemic basis for other agencies. NSW should differentiate the state from Commonwealth practice that typically involves the Office of the Australian Information

Commissioner releasing a brief statement that an investigation was conducted and problems will not recur. The inadequacy of such reporting may be attributable to under-resourcing of the OAIC rather than its inward-looking corporate culture but is contrary to public trust.

Apology

As data custodians who serve the public interest and who often collect, process and share data on a mandatory basis it is incumbent on government agency to acknowledge mistakes. One starting point is an apology from the relevant Minister for particular incidents. That apology will be welcomed by the community if it is substantiated through process improvement.