A FUNDAMENTAL RIGHT TO THE PROTECTION OF YOUR PERSONAL INFORMATION THAT IS COLLECTED BY GOVERNMENTS: REVIEW OF THE NEW INFORMATION PRIVACY ACT 2014 (ACT)

BELINDA CHAPMAN*

ABSTRACT

Privacy is an emerging and important area of law. Never has it been as important as it is now for the Australian community to have confidence that the information their governments collect is being adequately used and protected. This is largely due to the advanced ability for people to access information, which has resulted in a heightened risk for information to spread widely, and at a speed not envisaged even five years ago. With recent privacy breaches, such as the inadvertent release of the personal information of approximately 10,000 detainees on the Commonwealth's Department of Immigration and Border Protection's website[1] the protection and use of personal information is a critical consideration for all governments. This article will examine the recently passed Information Privacy Act 2014 (ACT) by the ACT Legislative Assembly and will compare the Information Privacy Act 2014 (ACT) with the Privacy and Data Protection Bill 2014 (Vic)[2] recently tabled in Victoria which brings together privacy and law enforcement data security legislation. This article will compare governmental reports handed down in Victoria and the ACT, which addressed similar issues of data security and protection and made similar recommendations.

I INTRODUCTION

Privacy law has received attention in recent years and community views should not be underestimated. It is natural to be curious about the personal information of others and unfortunately this can result in the release of personal information through means such as inadvertent release; breaches on part of government officials or information security systems that are vulnerable to external attacks. In an age where the media is making profits from sources such as the very high profile WikiLeaks[3] it is not

* Belinda Chapman is an experienced public servant who has an interest in administrative law, freedom of information, privacy and access law. She is also an undergraduate student at the University of Canberra.

1 KPMG, *Management initiated review, Privacy breach – Data management, Abridged Report, Department of Immigration and Border Protection* (2014) <http://www.immi.gov.au/pub-res/Documents/reviews/kpmg-data-breach-abridged-report.pdf 4.

2 Privacy Data and Protection Bill 2014 (Vic).

3 WikiLeaks (2014) https://wikileaks.org/.

surprising that there has been a shift in an individual's attitude. This point was made by Simon Davies in a recent paper[4]

> …increased awareness of the importance of accountability, transparency and the rule of law with regard to both the activities of security agencies and the value of privacy. This shift - in many parts of the world - has empowered civil society, created a resurgence of interest in legal protections and sensitised media to key issues that have hitherto escaped public scrutiny at any substantial level.[5]

In Australia we are starting to see changes reflected in law arising from the 2008 Australian Law Reform Commission (ALRC) Report.[6] The Report extensively reviewed privacy laws across the Commonwealth as well as other jurisdictions and made recommendations. One of the key messages to come out of the consultation which informed the Report was that '…Australians do care about privacy, and they want a simple, workable system that provides effective solutions and protections.'[7]

The Commonwealth Government is implementing the recommendations in tranches and this year the Australian Privacy Principles (APPs) were enacted.[8] The APPs are a single set of privacy principles which have replaced the Commonwealth National Privacy Principles (NPPs) and the Information Privacy Principles (IPPs).[9] The APPs were drafted to:

> …reflect the information lifecycle – from openness and transparency in personal information handling practices, collection, notification and through to disclosure, quality and security, to access and correction.[10]

The drafters took note of the message to have a workable system and the APPs were drafted to '…simplify privacy obligations and reduce confusion and duplication.'[11]

The ACT Government and the Commonwealth have a longstanding relationship in relation to IPP compliance. The passing of the *Information Privacy Act 2014* (ACT) sees the introduction of a set of independent privacy principles, which were envisaged 20 years ago. This article will firstly review contemporary community expectations with regards to the protection of personal information. Secondly, the article will briefly analyse privacy protection in the national context. Thirdly, the article will

---

4 Simon Davies, The Privacy Surgeon, *A Crisis of Accountability, A global analysis of the impact of the Snowdon revelations* (2014) 5.

5 Ibid.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* Report No 108 (2008).

7 Australian Law Reform Commission, *Privacy Law and* Practice (2012) http://www.alrc.gov.au/inquiries/privacy.

8 *Privacy Act 1988 (*Cth) Schedule 1.

9 Timothy Pilgrim, 'Privacy Reform — Act Three' (Speech delivered at the iappANZ 'Privacy Unbound' summit, Sydney, 25 November 2013) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-reform-act-three>.

10 Ibid.

11 Ibid.

review the relationship between the ACT Government and the Commonwealth and review the *Information Privacy Act 2014* (ACT) and its implementation.

The article will then review the findings from the Victorian Auditor-General's Report *Maintaining the Integrity and Confidentiality of Personal Information*[12] and the ACT Auditor-General's Office Performance Audit Report *Whole of Government Information and Communication Technology Security Management and Services*[13] as well as a Report by Allan Hawke, *Governing the City State, One ACT Government – One ACT Public Service'*[14] which addressed similar themes. The article will conclude with a view on whether the ACT Government missed an opportunity by not considering a similar regime to the one the Victorian Government are pursuing.

II OAIC SURVEY OF COMMUNITY EXPECTATIONS: HOW IMPORTANT IS PRIVACY?

In recent years the soon to be abolished Office of the Australian Information Commissioner (OAIC) has played a role in the oversight of Commonwealth information policy. Part of that role is to conduct regular surveys and inquiries and report to the Australian Government. In 2013 the OAIC released a Report, *Community Attitudes to Privacy Survey.*[15] The Report set out to capture '…Australians' changing awareness and opinions about privacy, as well as their expectations in relation to the handling of their personal information.'[16] The Report made findings on other privacy issues such as privacy in the cyber world.[17]

One of the key findings was that almost half of our population view online services as the biggest risk to their privacy.[18] Sixteen per cent were concerned about data security and the Report also found that a quarter have concerns with identity theft/fraud.[19] The results may also diminish the view that young people accept the risks and enjoy sharing their personal information online on sites such as Facebook because the results indicate that 60 per cent of young Australians have concerns with privacy risks associated with their personal information and online services.[20] The

12 Victorian Auditor-General, Maintaining the Integrity and Confidentiality of Personal Information, Report No 2009-10.8 (2009).

13 ACT Auditor-General's Office Performance Audit Report, *Whole-of-Government Information and Communication Technology Security Management and Services,* Report No 2/21012 (2012).

14 Allan Hawke, Governing the City State, One ACT Government – One ACT Public Service, ACTPS Review Final Report (2011) < http://www.cmd.act.gov.au/__data/assets/pdf_file/0011/224975/Governing_the_City_State.pdf>.

15 Office of the Australian Information Commissioner, *Community Attitudes to Privacy Survey, Research Report* (2013) < http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/Final_report_for_WEB.pdf>.

16 Ibid 3.

17 Ibid.

18 Ibid.

19 Ibid.

20 Ibid.

Report also found that 33 per cent of our population have issues '…with the way their personal information was handled in the previous year.'[21] This figure may grow because there has been increases in privacy complaints and a large increase in data breach notifications.[22]

The results also indicate that 82 per cent of Australians are now aware of Federal privacy laws compared with 69 per cent in 2007[23] and 69 per cent of Australians trust the government more with their personal information than private entities.[24] While the figure of 69 per cent is reasonable, one can conclude from the overall results that Australians are aware of their privacy rights and have concerns about the way their information is handled, particularly because Australians are increasingly interacting with governments online.

III THE NATIONAL CONTEXT

The Northern Territory has an independent statutory body administered by the *Information Act 2002* (NT) and Queensland and New South Wales also have Information Commissioners.[25] Tasmania has an Ombudsman with powers to investigate privacy complaints[26] and in South Australia privacy protection is administered by way of compliance for government agencies with a set of administrative instructions through a Privacy Committee.[27] Western Australia has an Information Commissioner[28] and various privacy principles are provided for in the Western Australia freedom of information laws.[29] It appears that all jurisdictions cover the protection of privacy adequately, some better than others and I will analyse Victoria alongside the ACT as both jurisdictions are in the midst of privacy reform.

IV ACT GOVERNMENT AND THE PRIVACY ACT 1988

In 1994 the Commonwealth enacted laws through section 23 of the *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth) which provided for the Information Privacy Principles (IPPs) in the *Privacy Act 1988* (Cth)

---

21 Ibid.

22 Office of the Australian Information Commissioner, *Annual Report 2012-13* (2013) 4 <http://www.oaic.gov.au/images/documents/about-us/corporate-information/annual-reports/Annual-report-2012-13/Complete_pdf_AR_2012-13.pdf> There was a 10.2% increase in privacy complaints and a 33% increase in data breach notifications for the 2012-13 financial year. Note, this is not taking the Commonwealth Ombudsman's complaints into account.

23 Office of the Australian Information Commissioner, *Annual Report 2012-13* (2013) 4 <http://www.oaic.gov.au/images/documents/about-us/corporate-information/annual-reports/Annual-report-2012-13/Complete_pdf_AR_2012-13.pdf> 4.

24 Ibid 5.

25 *Privacy and Personal Information Protection Act 1998* (NSW); *Right to Information Act 2009* (Qld) and *Information Privacy Act 2009* (Qld).

26 *Personal Information and Protection Act 2004* (Tas).

27 Government of South Australia State Records, *Recording Government, Privacy Committee of South Australia* (2014) http://www.archives.sa.gov.au/privacy/committee.html.

28 *Freedom of Information Act 1992* (WA) ss 55-64.

29 *Freedom of Information Act 1992* (WA).

to apply to ACT Government agencies. When the amendments were drafted the application of the IPPs were not intended to be a long term solution. The Bill described the arrangement as '…on an interim basis until an ACT enactment provides otherwise, the application of the Information Privacy Principles in the Privacy Act to ACT public sector agencies.'[30]

With the extensive promotion of privacy law in the Commonwealth context, it is not surprising that the ACT has taken the opportunity to enact its own stand-alone Act. The Attorney-General, Simon Corbell MLA, acknowledged the ALRC Report's[31] key recommendations and the enactment of the Commonwealth's *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), which were designed to implement the first tranche of recommendations made in the Report.[32]

As noted previously, the APPs replaced the IPPs and NPPs and were not drafted in a way to apply to ACT Government agencies. It is unclear whether this was an oversight or was intended at the time of drafting because of the *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (ACT), ACT Government agencies would continue to adhere to the IPPs from 12 March 2014.[33]

A *Overview of the Information Privacy Act 2014 (Act)*

The *Information Privacy Act 2014* (ACT) was drafted in accordance with commitments the ACT Government took to the 2008[34] and 2012 ACT Legislative Assembly elections, and its intention is said to be connected to s 12 of the *Human Rights Act 2004* (ACT) whereby everyone has a right to privacy protection and that their information will not be interfered with in an unlawful manner.[35] This is said to be based on Article 7 of the United Nations International Covenant on Civil and Political Rights.[36] However, the *Information Privacy Act 2014* (ACT) does expressly mention it in the objects.[37] The supplementary explanatory memorandum explained human rights protection and the connection to Article 7 of the United Nations International Covenant on Civil and Political Rights:

30 Explanatory Memorandum, Australian Capital Territory Government Service (Consequential Provisions) Bill 1994 (Cth) 3.

31 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* Report No 108 (2008).

32 Explanatory Memorandum, Information Privacy Bill 2014 (ACT) 2.

33 *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (ACT) s 23.

34 http://treasury.act.gov.au/documents/Summary%20of%20Election%20Commitments%20(17%20Oct).pdf 9. The ACT Government committed funding to develop a Privacy Act.

35 Revised Explanatory Memorandum, Information Privacy Bill (ACT) 3.3.

36 Ibid.

37 *Information Privacy Act* 2014 s 7. Section 2A(h) of the *Privacy Act 1988* (Cth) sets this out in its objects.

> …Bill supports and enhances the right to privacy by ensuring that there is a clear framework setting out how ACT public sector agencies collect, use, disclose and otherwise manage personal information.'[38]

The *Information Privacy Act 2014* (ACT) is well drafted and clearly sets out how the ACT Government must collect, use and disclose and manage personal Information.[39] The 'Territory privacy principles' (TPPs)[40] mirror the APPs as set out in Schedule 1 of the *Privacy Act 1988* (Cth).[41] The ACT Attorney-General said that as a result of the passing of the privacy laws personal privacy will be better protected and like the APPs stated the passing of the *Information Privacy Act 2014* (ACT) '…promotes the protection of individual privacy by regulating the handling and management of personal information by ACT public sector agencies.'[42] A media statement released by the Attorney-General provided the following insight:

> …technological changes have led to a shift in community perceptions of privacy, people are more willing to share personal information but are also increasingly interested in how their information is handled and managed.[43]

B *Implementation at a Time of Uncertainty in the Commonwealth Context*

Part 5 of the *Information Privacy Act 2014* (ACT) allows for the appointment of an 'Information privacy commissioner'.[44] The appointment of a privacy commissioner is similar to the *Australian Information Commissioner Act 2010* (Cth)[45] regime but allows for 7 year appointments[46] and has the flexibility for arrangements to be made for the appointment of a privacy commissioner of another jurisdiction to exercise the functions.[47] There has been no official announcement about an appointment of an 'Information privacy commissioner'[48] and the issue was raised in the debate of 3 June 2014 by opposition leader Mr Jeremy Hanson MLA, Shadow Attorney-General. The Shadow Attorney-General expressed concerns about the services that have been

38 Revised Explanatory Memorandum, Information Privacy Bill (ACT) 2.
39 *Information Privacy Act 2014* (ACT).
40 Ibid Schedule 1.
41 *Privacy Act 1988* (Cth) Schedule 1, Australian Privacy Principles.
42 Simon Corbell MLA, Attorney-General, 'New privacy law to protect personal information' (Media Release, 3 June 2014) http://www.cmd.act.gov.au/open_government/inform/act_government_media_releases/corbell/2014/new-privacy-law-to-protect-personal-information.
43 Ibid
44 *Information Privacy Act 2014* (ACT) s 26.
45 *Australian Information Commissioner Act 2010* (Cth) s 15.
46 *Information Privacy Act 2014* (ACT) s 27(1).
47 Ibid s 28.
48 Ibid s 26.

provided by the Commonwealth in this regard and how the abolishment of the OAIC may impact on the ACT budget.[49]

During the Assembly debate Mr Shane Rattenbury MLA stated that government officials from the Justice and community Safety Directorate (JACS) had assured Mr Rattenbury MLA that officials have '…spoken to the Privacy Commissioner and he has assured them that there is no impairment of his capacity to provide privacy services to the ACT.'[50]

V REVIEWS CONDUCTED IN THE ACT AND VICTORIA

When the *Information Privacy Act 2014* (ACT) is compared with the recent Privacy and Data Protection Bill 2014 tabled by the Victorian Government,[51] it appears that the ACT Government may have missed an opportunity to expand the scope of reform if they had considered reports provided to them: *Whole-of government Information and Communication Technology Security Management Services*,[52] and *Governing the City State – One ACT Government – One Public Service*. Both reports highlight issues which may have justified the existence a privacy and data protection commissioner in the ACT. An interesting comparison is observed with the recent privacy reform in both jurisdictions. The primary difference between the two is that the Victorian Privacy and Data Protection Bill seeks to implement important recommendations made by the Victorian Auditor-General.[53] The recommendations the Victorian Government is implementing include the establishment of merged body to have an oversight of privacy and data protection which will enforce the adoption of a 'the whole-of-government information security policies and standards.'[54] The Commissioner for Privacy and Data Protection[55] will also oversee the '…implementation of information security policies and standards and compliance with reporting compliance.'[56]

---

49 ACT, *Parliamentary Debates*, Legislative Assembly, 3 June 2014, 1639 (Jeremy Hanson MLA, Shadow Attorney-General) <http://www.hansard.act.gov.au/hansard/2014/week06/1639.htm>.

50 ACT, *Parliamentary Debates*, Legislative Assembly, 3 June 2014, 1639 (Shane Rattenbury MLA) <http://www.hansard.act.gov.au/hansard/2014/week06/1639.htm>.

51 Privacy and Data Protection Bill 2014 (Vic).

52 ACT Auditor-General's Office Performance Audit Report, *Whole-of-Government Information and Communication Technology Security Management and Services*, Report No 2/21012 (2012).

53 Victorian Auditor-General, *Maintaining the Integrity and Confidentiality of Personal Information*, Report No 2009-10.8 (2009).

54 Ibid x.

55 Privacy and Data Protection Bill 2014 (Vic) s 95.

56 Ibid.

A *ACT Auditor-General's Report*

Pursuant to s 17(5) of the *Audit-General Act 1996* (ACT), in 2012 the ACT Auditor-General's Office handed down a Performance Audit Report *Whole of Government Information Technology Security Management and Services.* The Report examined security management and services of whole-of-government information and communication technology.[57] The main objective of the audit was to examine whether '…administrative structures and processes for whole-of-government ICT policies and procedures are well defined, managed and communicated.'[58] The Report outlined the importance of protective security policies because it ensures that information is handed by the right people, and that access is granted at the right time and location and this is said to be an important aspect of '…an organisation's overall management system, based on business risk.'[59]

When the Report was handed down there was a set of guidelines named *Protective Security Policy and Guidelines* which was delivered through a committee named ACT Security in Government Committee (ACTSIGC). The leading agency was JACS and this Directorate administered the *Protective Security Policy and Guidelines* and were the leaders in the promotion of protection and security of the ACT government's information and assets.[60] The Report highlighted that it was not known how well understood the *Protective Security Policy and Guidelines* were and whether there were adequate checks and balances in place that would ensure agencies are complying. This could, in part, be addressed if whole-of-government- administrative structures and processes were better defined and readily available.'[61] It should be noted that the standards issued in the guidelines were not mandatory when this Report was released.[62]

The Report highlighted that of the ACT Government's 1,025 information management systems only five per cent had a system security plan and 2.4 per cent '…had a threat and risk assessment'.[63] It is not known whether these figures have improved since 2012 but at the time there was recognition of the adoption of 33 mandatory requirements for the Guidelines.[64]

---

57 ACT Auditor-General's Office Performance Audit Report, *Whole-of-Government Information and Communication Technology Security Management and Services*, Report No 2/21012 (2012) 1.1 3.

58 Ibid 1.11 4.

59 Ibid 1.3 3.

60 Justice and Community Safety: ACT Government, *Protective security* (2012) http://www.justice.act.gov.au/page/view/439/title/protective-security.

61 ACT Auditor-General's Office Performance Audit Report, *Whole-of-Government Information and Communication Technology Security Management and Services*, Report No 2/21012 (2012) 5.

62 Ibid.

63 Ibid 6.

64 Ibid 7.

At the time of the Report the responsibilities for ICT security management and services and information were spread across various agencies:

- Treasury Directorate administered the *Territory Records Act 2002* (ACT), the Shared Services Division and Shared Services ICT Security Section provided information and communication technology for the ACT public service.
- Justice and Community Safety Directorate – managed the Security and Emergency Management Branch (SEMB).
- All directorates and agencies administered policies and staff compliance for ICT.[65]

The Report made two main recommendations. The first was for the Shared Services Division of JACS to improve the management of whole-of-government security practices by way of making a formal arrangement of the relationship of the Security and Emergency Management Branches, and the Shared Services ICT Security Section.[66] The other part of the first recommendation was:

> …clarifying and documenting the roles and responsibilities of an ACT Government IT Security Adviser, the ACT Security in Government Committee and directorate Agency Security Advisers and their supporting communication processes.[67]

This was given a high priority by the Auditor-General.

The second recommendation provided for improvements in whole-of government security management practices, which included risk management. The Report recommended that this could be done by the establishment of procedures for compliance and reporting and surveys, the completion of a review of the *Protective Security Policy and Guidelines* to clarify the Commonwealth's mandatory requirements, and the inclusion of international standards.[68] At the time of the drafting of the Report, pursuant to s 18 of the *Auditor-General Act 1996* (ACT) a final draft was provided to the relevant agencies. Both the Director-General of JACS and under Treasurer (Shared Services) agreed to these recommendations. The Report stated:

> On 23 May 2012 the Security and Emergency Management Senior Officials Group accepted revised terms of reference for the ACT Security in Government Committee, following a review by the ACT Security in Government Committee. These revised terms of reference will include the role of "reviewing and updating the ACT Protective Security Policy and Guidelines" and a requirement to "provide an annual report to the Security and

65 Ibid 17-18.
66 Ibid 1.18 10.
67 Ibid.
68 Ibid 11.

> Emergency Management Senior Officials Group on agencies" compliance with the Protective Security Policy and Guidelines.

The ACT Government's online Protective Security page covers the ACT *Protective Security Policy and Guidelines* and it should be noted that it was last published on 7 May 2012 and it is not known how well this has been updated since.

In the Report JACS also acknowledged the recommendation concerning risk plans and compliance with information security obligations and guidance.[69] JACS agreed that it is an issue and advised that JACS would '…add to its risk management plan the risk of not keeping information security policy and procedures current.'[70]

B *Governing the State: One ACT Government – One ACT Public Service*

In 2010 then Chief Minister, Mr Jon Stanhope MLA announced a review of the ACT public service. The review was conducted by Allan Hawke and handed down 2011. The aim '…was to ensure the configuration of the ACT public sector remains appropriate for meeting the Government's needs and delivering its future agenda.'[71] One of the recommendations was to establish a Chief Information Officer (CIO) and the CIO would be based in the proposed Chief Minister's Department.[72] The role would oversee a whole-of-government policy for issues such as information communications technology, strategic information, freedom of information, record keeping and storage and access. It would also '…build a pool of business analysts and project management resources for ready deployment across the service for information and communications technology and business improvement projects.'[73]

Similar to the findings in the Auditor-General's Report, Hawke found that responsibilities for knowledge management governance was across various agencies and that the responsibilities should be centralised and administered by the CIO.[74] Given the size of the ACT compared with other larger jurisdictions, it would be a better use of resources to have one body that is responsible for:

> the strategic program for gathering, storing and sharing ACTPS data. It would be responsible for the end to end continuum of government information including the Territory Records Act, the FOI Act and other legislation relating

---

69 Ibid 11.

70 Ibid 12.

71 Allan Hawke, *Governing the City State, One ACT Government – One ACT Public Service, ACTPS Review Final Report* (2011) <http://www.cmd.act.gov.au/__data/assets/pdf_file/0011/224975/Governing_the_City_State.pdf>. Opening letter.

72 http://www.cmd.act.gov.au/open_government/what_is_open_government/about_the_gio. It should be noted that the ACT Government established the Government Information Office (GIO) and not the CIO as recommended in the Hawke Report.

73 Ibid 8.

74 Ibid 93.

> to record keeping by the ACTPS, the proactive release of government material, whole of government information management and ICT governance, policy, information architecture, strategic planning, and web 2.0 technologies.[75]

One deliverable under the Report was for the implementation of a knowledge management framework and a foundation of this was in an ICT strategic plan.[76] Following this recommendation, instead of establishing a CIO, the ACT Government established the Government Information Office (GIO). The role of the GIO is to '… provide across-government advice and coordination on ICT issues and release of government information.'[77] It is based in the Chief Minster, Treasury and Economic Development Directorate and works with ICT areas across the ACT Government.[78] It is not known why the ACT Government did not implement Hawke's recommendation 22 in full.[79] However, the ACT Government is proactive in their approach to innovation with technology[80] with initiatives such as the Strategic Plan for ICT 2011-15 which outlines a direction and objectives with ICT investment government on information security.[81]

VI AUDITOR-GENERAL REPORT VICTORIA 2009

Pursuant to s 16AB of the *Audit Act 1994* (Vic), the Victorian Auditor-General handed down a Report *Maintaining the Integrity and Confidentiality of Personal Information.* This Report focused on personal information and '…how it is stored, processed and communicated by the public sector. It evaluates whether its confidentiality and integrity has been maintained.'[82] The Report had a similar focus to the *Whole-of-Government Information and Communication Technology Security Management and Services* [83] and acknowledged the importance of the maintenance of confidentiality and that those who require the information are granted access, and that

---

75 Ibid.

76 Ibid 94.

77 Government Information Office, ACT Government, *About Us* (2014) <http://gio.act.gov.au/about/>.

78 ACT Government, Open Government, *About the GOI* (2012) http://www.cmd.act.gov.au/open_government/what_is_open_government/about_the_gio.

79 Allan Hawke, *Governing the City State, One ACT Government – One ACT Public Service, ACTPS Review Final Report* (2011) < http://www.cmd.act.gov.au/__data/assets/pdf_file/0011/224975/Governing_the_City_State.pdf> 8.

80 ACT Government, *The Strategic Plan for ICT 2011-15* (2012) http://www.cmd.act.gov.ay/_data/assests/pdf_file/0011/247826/The_Strategic_Plan_for_ICT_2011-15.pdf.

81 Ibid.

82 Victorian Auditor-General, *Maintaining the Integrity and Confidentiality of Personal Information*, Report No 2009-10.8 (2009) vii.

83 ACT Auditor-General's Office Performance Audit Report, *Whole-of-Government Information and Communication Technology Security Management and Services*, Report No 2/2012 (2012).

secure storage of personal information is maintained so '…that information provided is not later corrupted or lost, either intentionally or inadvertently.'[84]

The Auditor-General examined three departments and concluded that '…the ability to penetrate databases, the consistency in our findings and the lack of effective oversight and coordination of information security practices strongly indicate that this phenomenon is widespread.'[85] This is similar to findings in the ACT and the Report found that this problems was largely due to the '…security policy, standards and guidance for the sector are incomplete and too narrowly focused on ICT security.'[86]

The Auditor-General found that departments were not meeting their responsibilities in the context of maintenance and development of whole-of-government information security guides, and standards to improve culture and the provision of support and advice on developments in information security.[87] An interesting comparison with the ACT is that the risk management frameworks in both jurisdictions were considered not ideal. The Victorian Report found that '…greater guidance across the sector is needed. Risks cannot be managed where an agency is not aware of them, or does not understand their significance.'[88]

Whilst is cannot be determined how well the ACT Government have implemented the recommendations made in the 2012 Report, the Victorian Government have addressed many of the issues highlighted by way of the introduction of the Privacy and Data Protection Bill 2014 (Vic), which will ensure that the Victorian Government administers the personal information it collects in a consistent and secure manner.[89]

VII VICTORIAN PRIVACY DATA AND PROTECTION BILL 2014

The Victorian Attorney-General, Robert Clark MP released a press statement and explained that the intent of the Privacy and Data Protection Bill is to merge the roles of the Commissioner for Law Enforcement Data Security, and the Privacy Commissioner so there will be one body with oversight of data protection and privacy. The Attorney-General hopes that this approach will '…strengthen the protection of individuals' private information held by the Victorian public sector.'[90]

---

84 Victorian Auditor-General, *Maintaining the Integrity and Confidentiality of Personal Information*, Report No 2009-10.8 (2009) vii.

85 Ibid.

86 Ibid viii.

87 Ibid viii.

88 Ibid ix.

89 Robert Clark MP, Attorney-General, 'New framework for privacy and data protection and information sharing (Media Release, 12 June 2014) http://www.robertclark.net/news/new-framework-for-privacy-and-data-protection-and-information-sharing/.

90 Ibid.

The IPPs contained in the Privacy and Data Protection Bill largely mirror the Commonwealth APPs for the 'Fair Handling of Personal Information, on which the Commonwealth Government's private sector privacy legislation was also based originally.'[91] This will result in the Victorian IPPs coming more into in line with Commonwealth reforms. The order of the IPPs are somewhat different to the APPs. An illustration of this can be found by comparing APP 1,[92] with IPP 5 whereby the requirement for a privacy policy is set out in a separate principle, however, it is not as prescriptive as APP 1 which sets out obligations to handle personal information in a transparent way, and the requirements for a privacy policy.[93] The mandatory requirement for a privacy policy is an important aspect of privacy law so that the community can have a clear understanding of what its government is doing with a person's personal information and what a person is entitled to under law with respect to the handling and protection of their personal information as well as access to their personal information.

It is not known why the Victorian Government did not align the IPPs more closely to the Commonwealth APPs and as was done in the ACT, however, they generally cover the same themes to promote an open and transparent collection, use and disclosure of personal information throughout its lifecycle.

An important aspect of the Privacy and Data Protection Bill is contained in Part 4 – Protective Data Security. It provides discretion for the Commissioner for Privacy and Data Protection to issue a protective data security framework, the issue of data security standards and protective data security plans.[94] The issues raised in the Report[95] have been drafted into a legislative framework and the Commissioner for Privacy and Data Protection will have responsibilities for issuing protective security standards. The role of the office will also be to assist agencies to develop consistent plans. In a positive move by the Victorian Government, the Privacy and Data Protection Bill sets out mandatory compliance with the protective data security standards[96] and two years after the implementation of the protective data security standards agencies must have security risk assessments and a protective data security plan implemented, to ensure that the standards are applicable to that particular agency.[97] Another important aspect of the Privacy and Data Protection Bill is found in s 89 which sets out the risk and compliance issues that were raised in the Auditors-General reports in both the ACT and Victoria. There is also a requirement for the

91 Explanatory Memorandum, Privacy and Data Protect Bill 2014 (VIC) 2.
92 *Privacy Act 1988* (Cth) Schedule 1 APP 1.1.
93 Ibid.
94 Explanatory Memorandum, Privacy and Data Protect Bill 2014 (VIC) Part 4.
95 Victorian Auditor-General, *Maintaining the Integrity and Confidentiality of Personal Information*, Report No 2009-10.8 (2009).
96 Privacy and Data Protect Bill 2014 (VIC) s 88.
97 Ibid s 89.

protective data security plans to be reviewed every two years and reported to the Commissioner for Privacy and Data Protection.[98]

Overall, the Privacy and Data Protection Bill is an improvement on part of the Victorian Government because it brings together privacy laws with information security to adequately protect personal information. The Victorian Government is ahead of other Australian jurisdictions and it will be interesting to watch the progression of the Privacy and Data Protection Bill through Parliament.

VIII CHANGING THE ICT ENVIRONMENT IN THE ACT

In the recent 2014-15 ACT budget, the ACT Government announced that it is '…capitalising on opportunities in digital technology with initiatives that will transform the way individuals and businesses interact with the government and the world.'[99] The ACT Government intends to invest almost $85 million in digital technology[100] and this will include initiatives such as:

- automated accounts payable systems;
- replacement of the revenue collection system;
- an automated accounts payable system;
- a new court management system which will include infrastructure to allow for the filing of documents electronically;
- a system to allow for electronic tendering; and
- investment in the ACT Governments open data platform which will include making datasets more accessible.[101]

The Act Government are also planning to invest in the following:

- a combined private and public cloud service which will reduce data storage costs;
- improvements to the payroll and Human Resources systems;
- ACT public servants will be provided with IT self-help tools that are said to be an improvement on what they have; and
- a feasibility study to identify options for the digitisation of the records of the ACT Public Service.[102]

The distribution of the IT self-help tools is a positive move and there is sound investment in ICT infrastructure. However, as has been illustrated throughout this article, the ACT Government could have invested money in reviewing all the ICT services across the ACT Public Service and could have revisited Hawke's

98 Ibid 89(4).

99 C Capitalising on a Digital Technology – Digital Canberra < http://apps.treasury.act.gov.au/__data/assets/pdf_file/0020/601706/Digital-Canberra.pdf>.

100 Ibid.

101 Ibid.

102 Ibid.

recommendation to combine various services across all directorates that involve the collection, protection, storage and use of information into one body.

IX CONCLUSION

It appears the ACT Government has missed an opportunity to centralise information policy, information privacy law and data protection when they drafted the *Information Privacy Act 2014* (ACT) and perhaps it was another oversight when the recent 2014-15 budget was handed down. The ACT Government is heading in a positive direction with ICT data security initiatives and the passing of the *Information Privacy Act 2014* (ACT) but the co-ordination and centralisation of privacy and data protection security remains an issue. As a result of sound initiatives as outlined in this article it appears that the ACT Government may have basis for establishing an office with an independent Privacy and Data Protection Commissioner or the role of the GIO could be enhanced to include the information security functions as well. This would greatly improve the collection, storage and use of personal information across the ACT Public Service and address many issues raised in the Hawke and ACT Auditor-General's Reports, and the ACT would not have to rely on the Commonwealth for assistance.