Senator the Hon. Ian MacDonald
Chair
Senate Legal and Constitutional Affairs Legislation Committee
Parliament House
Canberra ACT 2600

By email: legcon.sen@aph.gov.au

Dear Senator MacDonald

Freedom of Information Amendment (New Arrangements) Bill 2014

Following the public hearing held by the Senate Legal and Constitutional Legislation Committee (the Committee) on Monday, 10 November 2014, I wish to draw to the Committee's attention some important considerations relating to proposed co-location of the Privacy Commissioner (the Commissioner) with the Australian Human Rights Commission (AHRC). These matters were touched on in the Office of the Australian Information Commissioner's (OAIC) submission to the Committee and also in my responses to questions at the hearing.

While I am committed to making any administrative arrangements work, it is my view that the Bill creates a model that is not suited to achieving the objectives of the *Privacy Act 1988 (Cth)* (the Privacy Act) in the most efficient way. A more effective model would be to return to a standalone Office as it was between 2000 and 2010. I say this because:

1. Historical experience indicates housing privacy within the AHRC is not the most effective model
2. The privacy functions are diverse and complex, warranting a single focus Commissioner with dedicated resources and full control over the use of those resources
3. Privacy legislation regulates personal information – a key asset of business, government and the information economy
4. Efficiencies in sharing corporate services including IT and human resources are already realised through a Memorandum of Understanding (MOU) between the OAIC and the AHRC, which I would intend to continue
5. Inclusion of the Privacy Commissioner as Human Rights Commissioner, required by the AHRC governance structure as outlined in the AHRC submission, would mean funds allocated to the privacy functions, and therefore the exercise of the privacy statutory functions, could be subject to agreement and direction by the President and other members of the AHRC.

History of privacy administrative arrangements with the AHRC

Privacy regulation began with a Privacy Commissioner being part of the then Human Rights and Equal Opportunity Commission (now the AHRC). However, in 2000 the Privacy Commissioner was separated off and a separate Office of the Privacy Commissioner was created. This coincided with amendments to the Privacy Act which brought in the private sector to the coverage of the Privacy Act. The separation was supported by the AHRC at the time.

In part, the reasons for the separation related to the significantly different regulatory focus of the Privacy Commissioner. There were challenges administering the diverse and complex privacy functions, conferred under a number of statutes, from within another agency with a different focus and approach. The size of the resources required to carry out the privacy functions, which made up a large component of the AHRC, versus the resources allocated to each of the human rights Commissioners, led to 'competition' for resources and focus which was another reason why the privacy function was moved out of the AHRC in 2000. I am concerned that this situation could be repeated under the proposed model.

Functions

The functions under the Privacy Act are diverse and complex (see Attachment). They have similarities with the Australian Consumer and Competition Commission (ACCC), Australian Securities and Investment Commission (ASIC) and the Australian Communication and Media Authority (ACMA), but with the addition of a sizable complaints function. These functions include:

- Regulation of the flow of personal information in the context of the information economy throughout Australia and in an international context
- Development of guidelines and legislative instruments for the application of the Privacy Act
- Provision of advice and responding to enquiries from entities and the public in respect of the application of the Privacy Act
- Regulating credit information throughout the economy under the credit provisions of the Privacy Act
- Complaints handling for allegation of breaches of the Privacy Act by individuals against entities covered by the Act, where the Commissioner seeks to conciliate but has the ability to determine the matter. Privacy complaints have increased by 183% in the past financial year (see workload statistics below).
- Commissioner initiated investigations (CII) most regularly used in the case of data breaches. These involve detailed investigations of organisations' often complex information security systems
- The Commissioner also has access to resolve such investigations through issuing a Determination, seeking enforceable undertakings or civil penalties
- Privacy Performance Assessments of entities covered by the Act in respect of both the Australian Privacy Principles and credit provisions
- Binding privacy Code development and approval – both voluntary, Commissioner requested and Commissioner initiated
- Privacy Impact Assessments – voluntary and involuntary

- Public Interest Determinations, where the Commissioner can through legislative instrument allow for an activity to occur that would otherwise constitute a breach of the Act
- Formal Recognition of External Dispute Resolution Schemes (EDR) and oversight of their activities in respect of handling privacy complaints in specific sectors.
- Providing advice to Government on the implications of various policy initiatives on the handling of personal information
- Significant amount of work undertaken under MOUs with government Agencies which require dedicated staff and expertise
- Education and awareness functions aimed at entities (both private and government sector) as well as the general community on their rights and responsibilities
- Various functions under a number of other statutes including the Crimes Act, Anti-Money Laundering/Counter Terrorism Financing legislation, Personal Property Securities, the Telecommunications Act, Data Matching Act and the Health Act
- The Commissioner is also the Privacy Commissioner for the Australian Capital Territory (ACT) under ACT legislation regulating ACT government agencies.

The economic impact of privacy functions

Privacy impacts on the whole economy and community. This can be summarised as follows:

- Privacy regulation is a significant economic issue as well as a human rights issue. In that regard, it is particularly sensitive as it regulates a key business asset of private sector organisations and government, the personal information of their customer base. Capacity building work with business and government requires trust that the Commissioner is independent and impartial in his/her approach to privacy and data protection issues in a co-regulatory context.
- Successive Commissioners have forged a positive working relationship with business and government, built on a balanced approach to data protection/privacy. This was done with the aim of reducing the regulatory burden on entities regulated by the Privacy Act and assisting government agencies to get the privacy aspects of new policy proposals right to ensure community trust, and importantly for business ensuring a level playing field. A single focus independent Commissioner is required in order to continue to build on this strength.
- The Privacy Act's statutory responsibilities requires an agency with staff who have a broad range of skills and resources to allow it to work closely with private sector organisations and government on complex technological business practices, processes and systems.
- Any proposed efficiencies in locating the Commissioner with the AHRC may not be realised given the complexity and size of the privacy functions and the growth in workload currently managed through efficiencies gained with specific skills and expertise.

Resourcing and Administration Issues

It is essential that the resources made available to the Commissioner, to undertake the privacy functions can be targeted (without the potential for dispersion across other functions) to ensure the greatest efficiency. The resources to undertake the privacy functions, under the proposed model, will ultimately be at the discretion of the President of the AHRC, and potentially subject to competing priorities.

It is also important to note that the OAIC currently has staff funded under MOU arrangements with other Agencies to provide privacy regulatory functions and services (for example functions under the PCEHR). The Commissioner is signatory to these MOUs and is responsible for the delivery of the agreed outcomes. It is therefore essential that the Commissioner has control over the resources tied to these MOUs to be able to fulfil the commitments under those agreements.

Privacy workload statistics

Finally, the following table outlines a selection of statistics showing a general increase in workload over the last four years in the privacy jurisdiction. For full statistics on other regulatory activities including development of guidance, regulatory instruments, advice and education and awareness activities, please see the OAIC's annual reports at www.oaic.gov.au.

	2010/11	2011/12	2012/13	2013/14
Web visits	1376498	1007262	1376498	1,510,859
Phone enquiries	10313	8976	9009	11,737
Written enquiries	1690	1541	1567	2141
Complaints	1222	1357	1496	4,239
Commissioner Initiated Investigations and Data breach Notifications	115	83	74	78
Media enquiries	182	244	280	240

I would of course be available to elaborate on any of the points raised in this letter should the Committee wish.

Yours sincerely

Timothy Pilgrim
Australian Privacy Commissioner
11 November 2014

Health

- Personally Controlled Electronic Health Records (PCEHR) / Health Identifiers complaints investigations
- General health complaints, Data Breach Notifications (DBNs), Commissioner Initiated Investigations (CIIs), under the APPs.
- Mandatory PCEHR DBNS
- Development of Guidance and advice for the health sector.
- Privacy Assessments (audits)
- Approval of S.95, 95A, 95AA (Guidelines through the NHMRC) – medical research, health and genetic information
- S.135 (Health Act) – Guidelines on MBS/PBS

National Security Initiatives - Identity Security and Cyber Policy

- National Security Legislation, recent initiatives e.g. National Security Amendment Bills. Advice to Government, Parliament, oversight.
- Document Verification System: Conduct Assessments (audits) of issuing and user agencies: to be expanded to private sector, provide guidance on the privacy impacts and minimisation strategies on the use and extension of the DVS.
- Contribute to work of Federal / State National Identity Security Coordination Group in enhancing Australia's identity security framework.
- Contribute to cross government of Cyber Policy Group on Cyber Security.

Telecommunications

- Conduct assessments, Data Breach Notifications (DBNs), Commissioner Initiated Investigations (CIIs), individual complaints.
- Respond to formal consultation requirements in ACMA / Communications Alliance Telco Codes.
- Amendment to Telecommunications Act: expected to shift regulation to Privacy Act.
- Undertake s.309 assessments (audits) of disclosures to law enforcement agencies.
- Coordination of regulatory action with ACMA.
- Provide advice on privacy impacts of IPND, Do not call Register, interrelationship between Spam and Privacy Acts.

Regulatory, Guidance, Monitoring, Advice functions

- Administer Privacy Act, associated rules, binding guidelines, public interest determinations, and privacy codes.
- Handle privacy complaints from individuals in relation to Australian and Norfolk Island, ACT government agencies and organisations (all business sectors). Conduct Assessments (audits) of agencies, credit providers, credit reporting bodies and since the reforms, the private sector.
- Data Breach Notification (DBNs): conduct risk assessment, seek further information, provide guidance and consider for possible regulatory action.
- Commissioner Initiated Investigations (CIIs): conduct investigations including use of new regulatory powers (enforceable undertakings, make determination, civil penalties).
- Direct government agencies to conduct a Privacy Impact Assessment.
- Make Public Interest Determinations to exempt otherwise unlawful acts and practices in the public interest: legislative instrument requires consultation, approval, registration.
- Make APP Codes: legislative instrument requires consultation, approval, registration.
- Guidance related functions (making guidelines and developing resources for the avoidance of interferences with privacy, promoting understanding of the Privacy Act and delegated legislation, undertaking educational programs to promote protection of privacy).
- Monitoring related functions (for example, examining proposed enactments that would require or authorise interference with privacy).
- Advice related functions (providing advice to agencies and organisations on the operation of the Privacy Act, reports and recommendations to Minister).

Cross Border Enforcement: participation in international forums

- APEC Cross Border Privacy Enforcement Agreement
- Asia Pacific Privacy Authorities
- OECD Global Privacy Enforcement Network

Code Development
Australian Privacy Principle (APP) Codes
Approve Codes under APPs.
Code regulator functions.

Data Matching

- Conducting audits of application of the Data Matching Act by DHS (statutory data matching using the TFN).
- Issuing Guidelines for voluntary data matching (that does not use the TFN).
- Examining data matching protocols developed by agencies (eg ATO, DHS) and considering requests for exemption from the voluntary guidelines.

Privacy Act
Privacy Commissioner Functions and interaction with other statutes and entities.

Credit Information

- CR Code (approval process, oversight and review)
- Issuing Credit rules
- External Dispute Resolution (EDR) scheme –recognition/ oversight – complaints
- Complaints, DBNs, CIIs
- Assessments (Audits)
- S20z (destroy credit info)
- Consumer, credit provider and credit reporting bodies advice and guidance

Crimes Act (Spent convictions)

- Handle complaints re spent convictions provision of Crimes Act
- Provide advice on privacy impacts of spent conviction regime

State and Territory Cooperation
Working with State and Territory Privacy Commissioners

Personal Property Securities Register (PPSR)

Entities and individuals, that may not otherwise be covered by the Privacy Act, are covered for specific acts (unauthorised searches and not giving appropriate notices). All regulatory functions attributed.

Australian Capital Territory (ACT)
Privacy Commissioner Functions for the ACT

Unique Student Identifier
Oversight functions

Public Interest Determinations
Advice on applications, public consultation process, approving, registration as legislative instrument

Submissions and Advice
To Parliamentary Committees and Government on issues relating to proposals impacting on the community's privacy

Small Business - Opt-in Register
Small business can opt in to be covered by the privacy Act.
Administering scheme, regulating small business

APPS – Government & business

- Guidelines
- Rules
- Advice
- Complaints
- Commissioner initiated investigations
- Assessments
- Data Breach Notifications
- Privacy Impact Assessments – Directing Agencies
- External Dispute Resolution Scheme oversight

Customs MOU

Oversight/audit of handling of passenger name records in accordance with International Treaty

Tax File Numbers (TFN)

- Issue TFN Rules
- Examine records of ATO
- Advice on policy proposals to extend use of TFN eg locating lost superannuation

Anti-Money Laundering and Counter Terrorism Funding Legislation (AML/CTF) and AUSTRAC

- Entities that may not otherwise be covered by the Privacy Act are covered where they have AML / CTF obligations. All regulatory functions attributed.
- Providing guidance to AUSTRAC on privacy impacts of their activities.