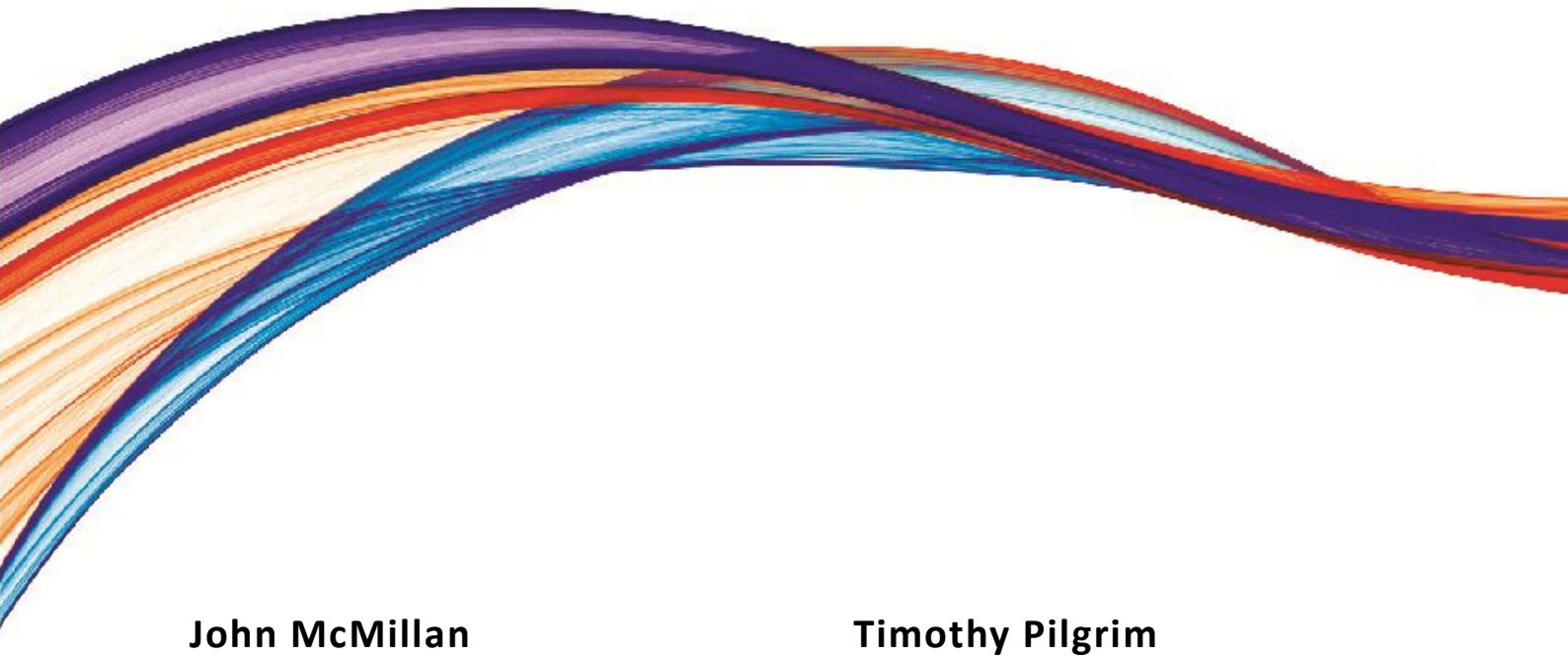
Australian Government

Office of the Australian Information Commissioner

Review of counter-terrorism legislation

Submission to the Council of Australian Governments

September 2012



John McMillan
Australian Information Commissioner

Timothy Pilgrim
Privacy Commissioner

Contents

Introduction **1**

Office of the Australian Information Commissioner **2**

Background to this Review **3**

The 4A framework **4**

Are the laws necessary and proportionate? **4**

Appropriate safeguards **5**

Accountability and appraisal 5

Privacy Act coverage 5

Comments on specific pieces of legislation **6**

Control orders and preventative detention orders – Division 104 and 105 of the *Criminal Code Act 1995* (Cth) 6

Conclusion **7**

Introduction

The Office of the Australian Information Commissioner (OAIC) thanks the Council of Australian Governments (COAG) for the opportunity to comment on the Review of counter-terrorism legislation (the Review).[1]

In formulating this submission, the OAIC draws on its previous public submissions, and submissions of the former Office of the Privacy Commissioner, to inquiries in relation to counter-terrorism laws, including:

- Inquiry into Terrorism Bills, submission to the Senate Legal and Constitutional Legislation Committee, April 2002
- Inquiry into the provisions of the Anti-Terrorism Bill (No. 2) 2005, submission to the Senate Legal and Constitutional Legislation Committee, November 2005
- Review of security legislation relating to terrorism, submission to the Security Legislation Review Committee (established under the Security Legislation Amendment (Terrorism) Act 2002), January 2006
- Inquiry into the Independent Reviewer of Terrorism Laws Bill 2008 [No. 2], submission to the Senate Legal and Constitutional Committee, September 2008
- Inquiry into the National Security Legislation Monitor Bill 2009, submission to the Senate Standing Committee on Finance and Public Administration, July 2009
- Inquiry into potential reforms of National Security legislation, submission to the Parliamentary Joint Committee on Intelligence and Security, 27 August 2012.[2]

The OAIC supports the goal of the Review to assess whether the counter-terrorism legislation specified in the Terms of Reference is necessary and proportionate and contains appropriate safeguards against abuse.[3] The OAIC considers that this Review presents an opportunity to examine whether the privacy interests of Australians receive an adequate level of protection in this context.

The central theme of privacy legislation (such as the *Privacy Act 1988* (Cth)) is to control how personal information is handled by government agencies and large businesses. The legislation does this by controlling what personal information can be collected, how it is to be used and managed, and when it can be disclosed or shared with others. A high proportion of the information collected by law enforcement agencies in their counter-

[1] http://www.coagctreview.gov.au/Pages/default.aspx
[2] Submissions are available on the OAIC website: www.oaic.gov.au/publications/submissions
[3] See Council of Australian Governments 2012, *Terms of Reference – Council of Australian Governments' (COAG) Review of Counter-Terrorism Legislation*, available at http://www.coagctreview.gov.au/about/Pages/default.aspx

terrorism activities is personal information. State law enforcement agencies are not subject to the *Privacy Act 1988* (Cth) (the Privacy Act), and state and territory privacy legislation varies in the level of protection that it provides. This should not carry the implication that the general privacy principles that underpin privacy legislation in Australia should be set aside. The OAIC will not comment at length in this submission on the detail of the counter-terrorism laws being examined by the Review. This submission will instead comment generally on how privacy principles should be considered in assessing the content and administration of counter-terrorism laws, with particular attention to the question of the proportionality and necessity of the specified counter-terrorism laws within a privacy framework. The submission will also focus on key privacy areas that may impact on the Review Committee's assessment of whether appropriate safeguards against abuse are in place.

The OAIC notes that the scope of its submission is limited to matters relevant to the privacy issues that are regulated under the Privacy Act.

Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner (the OAIC) was established by the *Australian Information Commissioner Act 2010* (Cth) (the AIC Act) and commenced operation on 1 November 2010. The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner. The former Office of the Privacy Commissioner was integrated into the OAIC on 1 November 2010.

The OAIC brings together the functions of information policy and independent oversight of privacy protection and freedom of information (FOI) in one agency, to advance the development of consistent workable information policy across all Australian government agencies.

The Commissioners of the OAIC share two broad functions:

- the FOI functions, set out in s 8 of the AIC Act — providing access to information held by the Australian Government in accordance with the Freedom of Information Act 1982 (Cth), and
- the privacy functions, set out in s 9 of the AIC Act — protecting the privacy of individuals in accordance with the Privacy Act and other legislation.

The Information Commissioner also has the information commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

The Privacy Act contains eleven Information Privacy Principles (IPPs) which apply to Australian and Australian Capital Territory Government agencies.[4] It also includes ten National Privacy Principles (NPPs) which apply to all businesses with an annual turnover of more than $3 million and some small businesses.[5]

The IPPs and NPPs are high-level principles which provide the minimum privacy standards with which agencies and organisations must comply when handling personal information. 'Personal information' is defined as 'information or an opinion... whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.'[6]

Background to this Review

The Prime Minister of Australia recently announced the start of the Council of Australian Governments' Review of counter-terrorism legislation. The role of the Review is to evaluate the operation, effectiveness and implications of key Commonwealth, State and Territory counter-terrorism laws.

Following the September 11, 2001 terrorist attacks in the United States and the 2005 terrorist attacks in London, the Commonwealth, State and Territory Governments enacted a series of laws intended to strengthen Australia's counter-terrorism laws. At the Special Meeting on Counter-Terrorism on 27 September 2005, the Council of Australian Governments (COAG) agreed that it was appropriate for these laws to be formally reviewed after a period of five years.[7]

The Review is being conducted by a six member Committee (the Review Committee), which has undertaken to provide a written report to COAG within 6 months of commencing the Review.

The Terms of Reference for the Review specify particular pieces of legislation that will be examined, and direct the Review Committee to make recommendations on whether these laws:

- are necessary and proportionate
- are effective against terrorism by providing law enforcement, intelligence and security agencies with adequate tools to prevent, detect and respond to acts of

[4] Section 14 of the *Privacy Act 1988* (Cth)
[5] Sections 6C, 6D and Schedule 3 of the *Privacy Act 1988* (Cth)
[6] Section 6 of the *Privacy Act 1988* (Cth)
[7] See Council of Australian Governments 2012, *Terms of Reference – Council of Australian Governments' (COAG) Review of Counter-Terrorism Legislation*, available at http://www.coagctreview.gov.au/about/Pages/default.aspx

terrorism

- are being exercised in a way that is evidence-based, intelligence-led and proportionate, and
- contain appropriate safeguards against abuse.[8]

The 4A framework

As one means of assessing whether laws relating to law enforcement and national security are necessary and proportionate, taking into account privacy considerations, the OAIC has developed a tool called the '4A framework' (see **Annexure A**).[9]

The 4A framework is intended to assist government agencies to consider personal information handling issues in their legislative measures specifically relating to new law enforcement or national security powers. The OAIC suggests that the issues identified in the 4A framework will be equally applicable in assisting the Review Committee to assess whether the counter-terrorism legislation the subject of the Review is effective, necessary and proportionate, and whether there are adequate privacy protections in place.

The 4A framework is underpinned by the recognition that measures that diminish privacy should only be undertaken where these measures are:

- necessary and proportional to address the immediate need, and
- subject to appropriate and ongoing accountability measures and review.

Are the laws necessary and proportionate?

In Australia, the Privacy Act protects an individual's privacy in relation to their personal information. While no general right to privacy exists in domestic law, this right is enshrined in Article 17 of the International Covenant on Civil and Political Rights, to which Australia is a signatory. Given this, and the value that Australians generally attach to the protection of rights and freedoms, there is a certain level of community expectation about how governments exercise powers in relation to matters that would ordinarily be considered to be 'private'.

---

[8] See Council of Australian Governments 2012, *Terms of Reference – Council of Australian Governments' (COAG) Review of Counter-Terrorism Legislation*, available at http://www.coagctreview.gov.au/about/Pages/default.aspx

[9] Office of the Australian Information Commissioner 2011, *4A framework – A tool for assessing and implementing new law enforcement and national security powers*, available at http://www.oaic.gov.au/publications/privacy_fact_sheets/Privacy-fact-sheet3_4Aframework.pdf

The right to privacy is not absolute and must be balanced with the community's right to safety and security. Governments have an acknowledged duty to protect the community from acts of terrorism. However, this does not diminish the role played by privacy in democratic societies, and in particular the duty on governments to deal with personal information in a manner that is consistent with respecting individual dignity and autonomy.

Any law – such as a counter-terrorism law – that enables a government to collect and use personal information should achieve an appropriate balance, and meet the test of being both necessary and a proportionate response to the perceived threat or harm. Privacy rights should not give way to safety and security considerations unless there is a clear and appropriate policy basis for doing so.

The Review Committee is urged to consider whether any of the provisions under review that authorise the handling of personal information derogate from the privacy principles that underpin the Privacy Act and if so, whether there are other ways in which the policy objective of the legislation could be met. The Review should also take into account whether the laws, which were enacted in response to particular global threats, still require the same types of provisions that are privacy-intrusive.

Appropriate safeguards

Accountability and appraisal

The OAIC's 4A framework suggests that accountability processes should include 'independent complaint handling, monitoring, independent audit and reporting and oversight powers commensurate with the intrusiveness of the measures'. The 4A framework also highlights the need for periodic appraisal of the measures, so that measures that are no longer necessary can be removed and unintended or undesirable consequences rectified.

It is of particular importance with legislation of the kind that is the subject of this Review, that accountability and oversight mechanisms are ongoing and effective. Periodic reviews represent one appropriate mechanism of promoting such accountability, and are essential in ensuring that individuals' privacy rights are given due regard in relation to counter-terrorism initiatives.

Privacy Act coverage

The IPPs in s 14 of the Privacy Act regulate the personal information handling practices of Australian, ACT and Norfolk Island government agencies, including those with enforcement and regulatory functions. The acts and practices of Australia's intelligence

agencies are exempt from the Privacy Act.[10] Accordingly, any personal information collected, used or disclosed by these agencies when fulfilling their functions is not covered by the Privacy Act. Australian Government agencies or organisations that engage in an act or practice related to a record that has originated with or has been received from one of these agencies are also exempt from the operation of the Privacy Act. Further, the Privacy Act does not extend to State or Territory authorities. The privacy safeguards provided by State authorities, including State law enforcement agencies, will differ depending upon the level of privacy protection operating in the relevant jurisdiction.

The OAIC notes that the current fragmented approach to regulating the personal information handling practices of law enforcement agencies could lead to inconsistencies in the level of privacy protection afforded to personal information. The OAIC considers that greater consistency across the accountability framework for law enforcement agencies could be achieved by ensuring that counter terrorism legislation is underpinned by a common set of considerations that reflect Australian community expectations about how personal information is handled.

Comments on specific pieces of legislation

The OAIC's comments on the specific pieces of legislation under Review are limited to a small number of key issues from the former Office of the Privacy Commissioner's submission to the Senate Legal and Constitutional Legislation Committee inquiry into the provisions of the Anti-Terrorism Bill (No. 2) 2005.[11] The OAIC does not comment further on the operation of this legislation.

Control orders and preventative detention orders – Division 104 and 105 of the *Criminal Code Act 1995* (Cth)

The OAIC notes that privacy protections that have been incorporated into Division 104 and 105 of the *Criminal Code Act 1995* (Cth) in relation to the collection, use and retention of specified types of personal information, namely fingerprints and photographs collected under ss 104.5(3)(j), 104.5(3)(k) and 105.43. The requirement that fingerprints and photographs must only be used for the purpose of 'ensuring compliance with the relevant control order' or 'determining whether the person is the person specified in the order' seems consistent with the Privacy Act principles.[12]

[10] See s7 of the *Privacy Act 1988* (Cth)

[11] Office of the Privacy Commissioner submission to the Senate Legal and Constitutional Legislation Committee, Inquiry into the provisions of the Anti-Terrorism Bill (No. 2) 2005, November 2005 http://www.privacy.gov.au/materials/types/download/8609/6461

[12] Sections 104.22 and 105.44 of the *Criminal Code Act 1995* (Cth)

We reiterate the query from our 2005 submission regarding the length of time for which this information is retained: it is not clear from the *Criminal Code Act* or from the Explanatory Memorandum why the retention period has been prescribed as 12 months.[13] The OAIC supports the destruction of records when they are no longer required, and considers that the inclusion of a maximum period is useful. However, we suggest that the Review Committee consider whether this time period remains appropriate, or whether a shorter retention period would suffice. The OAIC also notes that the provision of a maximum retention period should not preclude the destruction of records within shorter timeframes if it is determined they are no longer required at an earlier stage.

The OAIC supports the requirements in ss 104.29 and 105.47 for the Attorney-General to report to Parliament annually on the operation of control orders and preventative detention orders (respectively) for the previous year. However, the OAIC notes that the *Administrative Decisions (Judicial Review) Act 1977* (Cth) does *not* apply to the decisions of the Attorney-General under s104.2 (interim control orders) and Division 105 (preventative detention orders).[14] We query the policy basis for the exclusion, and whether this provides a suitable level of accountability and transparency.

Conclusion

The OAIC is of the view that there should be an appropriate balance between security and privacy. Australia's counter-terrorism legislation has expanded government's powers to collect personal information about individuals, including by covert means. Any such expansion is likely to diminish, to varying degrees, the privacy rights of individuals by eroding their ability to control their personal information.

It is imperative that where the legislation reduces the privacy protections that the Australian community have come to expect it is demonstrably necessary and proportionate to the identified threat. Further, such powers must be accompanied by enduring, consistent and robust accountability and oversight mechanisms. Given that Australia's national security context is dynamic, periodic reviews of this legislation are essential to ensure that the necessity and proportionality requirements are met.

Finally, in the event that the Review Committee makes recommendations about changes to provisions in the counter-terrorism legislation that relate to the handling of personal information, the OAIC strongly recommends that the Review Committee further recommend that Privacy Impact Assessments (PIA) be conducted in relation to these changes. A PIA would provide an opportunity for detailed analysis of the privacy impacts

[13] See paragraph 22 of submission to the Senate Legal and Constitutional Legislation Committee, November 2005

[14] Schedule 1 (dab) and (dac) of the *Administrative Decisions (Judicial Review) Act 1977* (Cth)

of any proposed changes to the relevant counter-terrorism legislation and assist in identifying ways to minimise those impacts. By identifying any risks, or benefits, of particular information handling practices, a PIA can identify options to minimise privacy issues and improve privacy outcomes. The OAIC has produced a detailed Privacy Impact Assessment Guide, which it recommends to the Review Committee.[15]

[15] Office of the Australian Information Commissioner 2010, *Privacy Impact Assessment Guide*, available at http://www.oaic.gov.au/publications/guidelines/Privacy_Impact_Assessment_Guide.html