Australian Government

Attorney-General's Department

Attorney-General's Department

Submission to the Queensland Department of Justice and Attorney-General

Review of Right to Information and Privacy Laws

June 2014

Part 1—Introduction

The Attorney-General's Department (AGD) welcomes the opportunity to make this submission to the review of the *Right to Information and Privacy Laws* by the Queensland Department of Justice and Attorney-General. This submission addresses the purposes of review set out in paragraphs 192(2)(b) and (c) of the *Information Privacy Act 2009* (Qld) (IP Act) and question 2.0 in the *Review of the Information Privacy Act 2009: Privacy Provisions* discussion paper.[1] It is AGD's view that legislative amendment is required to provide a clear authority for Queensland agencies to share personal information with the Australian Security Intelligence Organisation (ASIO) to enable the performance by ASIO of its functions.

AGD is concerned to ensure that the legislative regime for the protection of personal information held by Queensland state entities should not impede the flow of information between those entities and ASIO when they cooperate to protect Australia, its people and its interests from threats to security. AGD supports national consistency in the ability of State agencies to disclose personal information to ASIO to enable ASIO to perform its statutory functions and the alignment of the IP Act with the *Privacy Act 1988* (Cth) (Privacy Act), specifically the exclusion of the disclosure of personal information to ASIO from the operation of IP Act.

This submission is divided into the following parts:

- Part 1—Introduction
- Part 2—ASIO's role and security intelligence
- Part 3—ASIO's use of personal information
- Part 4—Rationale for an exemption in Queensland privacy legislation
- Appendix 1: ASIO's accountability framework
- Appendix 2: How ASIO safeguards personal information

Part 2—ASIO's role and security intelligence

ASIO's roles and responsibilities are set out in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act). The ASIO Act provides that ASIO is responsible for the protection of Australia, its people and its interests from threats to 'security', whether directed from, or committed within, Australia or overseas. In this context, 'security' includes:

a. The protection of, and of the people of, the Commonwealth and the States and Territories from:
    i. espionage
    ii. sabotage
    iii. politically motivated violence
    iv. promotion of communal violence
    v. attacks on Australia's defence system, or

[1] Queensland Department of Justice and Attorney General, *Review of the Information Privacy Act 2009: Privacy Provisions*, discussion paper, August 2013, p 10.

vi. acts of foreign interference

whether direct from, or committed within, Australia or not, and

b. The protection of Australia's territorial and border integrity, and

c. The carrying out of Australia's responsibilities to any foreign country in relation to the matters mentioned above.[2]

ASIO's key functions include collecting, analysing and evaluating intelligence relevant to security and providing advice to Ministers, Commonwealth and State authorities and other entities approved by the Attorney-General. The Australian Government and the governments of the States and Territories use security intelligence provided by ASIO to pursue and protect the national interest and to inform decision-making.

Security intelligence is vital to protecting Australia, its interests and its people. ASIO's role as Australia's security service is anticipatory and protective in nature – ASIO is expected to anticipate the actions of those who would harm us and act to prevent such harm. Access to personal information held by Queensland State entities is important in assisting ASIO in its role.

The performance of ASIO's role in Queensland is particularly relevant in light of upcoming major events to be hosted in Queensland, particularly, the G20 Leaders' Summit to be held in Brisbane in November 2014, the Asian Soccer World Cup and Cricket World Cup in 2015 and the Commonwealth Games in 2018.

Part 3—Why ASIO needs access to personal information

Access to personal information is critical in enabling ASIO to perform its legislated functions. Access to information, including personal information, enables ASIO to identify and locate persons of security concern and to determine their relevance to security. ASIO seeks information relevant to security from a variety of sources, including other authorities of the Commonwealth, agencies and police forces of States, authorities of other countries, private organisations and individuals. Information obtained through cooperation with other authorities is a key component of almost all security investigations.

Determining identity is key in this process and ASIO relies on cooperation with State and Territory agencies to access vital information that is not otherwise held by Commonwealth agencies. Analysis of personal information obtained through cooperation can remove the need to use more intrusive methods of investigation to determine security relevance. To obtain the same information by other means would likely require higher levels of intrusion into a person's privacy.

Under the ASIO Act, ASIO may, consistent with its statutory functions, communicate intelligence relevant to security for purposes relevant to security. Only the Director-General or persons authorised by the Director-General may communicate intelligence. Unauthorised communication of ASIO information by its officers or persons who have entered into a contract, agreement or arrangement with ASIO constitutes an offence. The communication of information by ASIO to foreign authorities is governed by legislation and internal policies and procedures and the propriety of such communications are regularly reviewed by the Inspector General of Intelligence and Security (IGIS).

---

[2] See the definition in section 4 of the *Australian Security Intelligence Organisation Act 1979*.

Part 4—Rationale for an exemption in Queensland privacy legislation

AGD is concerned to ensure that the legislative regime for the protection of personal information held by Queensland entities subject to the IP Act should not prohibit the flow of information between Queensland agencies and ASIO when they cooperate to protect Australia, its people and interests, from threats to security.

Clarity about permitted disclosures by State agencies of personal information is essential so that agency staff and the public whose personal information is held by those agencies clearly understand the circumstances in which personal information may be disclosed to ASIO.

International standards for privacy regulation recognise the need to balance the interests of individual privacy with the interests of national security by providing exceptions to the application of privacy principles where it is for the purpose of protecting national security.[3]

The IP Act's effect on Queensland entities' ability to share personal information with ASIO can be contrasted with the position in other Australian jurisdictions:

- under subsection 7(1A) of the Privacy Act, the disclosure of personal information made by a relevant agency to ASIO is exempt from the operation of that legislation, and
- under Victorian, Tasmanian and Northern Territory laws, the disclosure of personal information made by a State or Territory agency to ASIO is permissible where the disclosure is connected with the performance by ASIO of its functions, to an officer who is authorised in writing.[4]

AGD supports national consistency in State agencies' ability to disclose personal information to ASIO to enable ASIO to perform its statutory functions and considers that alignment with Privacy Act in this respect would be appropriate. In Report 108, *For Your Information: Australian Law and Practice* (2008),[5] the Australian Law Reform Commission (ALRC) considered that the current exemptions that apply to intelligence and defence agencies under the Privacy Act should remain, noting that stakeholders had commented that the exemptions acknowledged the need to balance the interests of individual privacy with the interests of national security and defence. For that reason, the exemption set out in subsection 7(1A) of the Privacy Act is our preferred model of exemption.

---

[3] Organisation for Economic Cooperation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 4; Memorandum, [46]; European Parliament, *Direction on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995), arts 3 (2), 13; recitals 16, 43; Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13].

[4] See the *Information Privacy Act 2000* (Vic); *Personal Information Protection Act 2004* (Tas); and *Information Act 2002* (NT).

[5] See note 6.

Appendix 1: ASIO'S ACCOUNTABILITY FRAMEWORK

ASIO is subject to robust accountability and oversight mechanisms. While ASIO is exempt from the operation of the Privacy Act, other accountability principles and oversight mechanisms address privacy issues, including:

- **Legislation** governing Australia's intelligence community and balancing of collective security rights and the rights of citizens, including to privacy, including:
  - *Australian Security Intelligence Organisation Act 1979*
  - *Telecommunications (Interception and Access) Act 1979*
  - *Archives Act 1983*
  - *Crimes Act 1914*
  - *Inspector-General of Intelligence and Security Act 1986*
  - *Financial Management and Accountability Act 1997*
  - *Intelligence Services Act 2001*
  - *Work Health and Safety Act 2012*, and
  - *Public Interest Disclosure Act 2013.*
- **Parliamentary oversight** of intelligence activities, including:
  - ASIO's annual report to the Parliament
  - Parliamentary Joint Committee on Intelligence and Security
  - Briefings of the Leader of the Opposition
  - Senate Estimates, and
  - Portfolio Budget Statement.
- **Ministerial accountability** ensuring clear lines of accountability, including:
  - Attorney-General's Guidelines on security intelligence
  - ASIO's classified Annual Report to the Attorney-General and Ministers
  - Briefings to the National Security Committee of Cabinet
  - Approval by the Attorney-General to use ASIO's intrusive warrant powers (and in the case of questioning and detention powers, approval of a judicial officer)
  - Approval by the Attorney-General for ASIO to liaise with international partners
  - Reporting to the Attorney-General on the value and intelligence obtained from each warrant, and
  - Regular advice and reporting to the Attorney-General.
- **Independent oversight**, including:
  - IGIS
  - Australian National Audit Office
  - Independent Reviewer of Adverse Security Assessments

- Security Appeals Division of the Administrative Appeals Tribunal
- Judicial review, and
- Review by the AGD of each case ASIO submits for a warrant to ensure it meets the legislative test.

These elements are designed to ensure a maximum degree of transparency, consistent with the requirements of national security.

Further disclosures of classified material are provided to the above bodies, for example:

- ASIO provides the Attorney-General and Ministers with a national security classified annual report detailing ASIO's outcomes and performance, and the Attorney-General subsequently tables an unclassified version in Parliament
- The IGIS provides national security classified advice on outcomes of inspections and inquiries to ASIO and the Attorney-General. The IGIS also provides an annual report of these activities to parliament, and
- The Parliamentary Joint Committee on Intelligence and Security conducts an annual review of administration and expenditure of intelligence agencies. The Committee has access to national security classified material and briefings to inform its report to the Parliament.

While the detailed breakdown of ASIO's expenditure is not publicly available, aggregate information appears in the Portfolio Budget Statement, and financial statements audited by the Australian National Audit Office are published in ASIO's annual report to Parliament.

Some elements of ASIO's accountability mechanisms are by necessity maintained in private, such as ASIO's reports to the Attorney-General on the value and intelligence from each warrant, briefings to Cabinet and briefings to the Leader of the Opposition.

This balance of public and private accountability measures is right for an intelligence organisation needing to maintain secrecy of its sources, methods, and operational capabilities so as to protect Australians from harm.

The IGIS

The IGIS is an independent statutory officeholder, appointed by the Governor-General, who is responsible for the oversight and review of the Australian intelligence community, including ASIO, in four main areas:

- compliance with the law
- compliance with ministerial directions and guidelines
- propriety, and
- respect for human rights.

The IGIS conducts independent enquiries, investigates complaints, makes recommendations to government and provides annual reports to the Parliament. When exercising her inquiry function, the IGIS has significant powers, comparable to those of a royal commission, to obtain information, require persons to answer questions and produce documents, take sworn evidence and enter the premises of any intelligence or defence intelligence agencies. In its submission to the 2008 Australian Law Reform Commission's review of Australian privacy law, the IGIS noted that the

Australian intelligence agencies are subject to privacy requirements that are informed by the principles that underpin the Privacy Act; and they are subject to a robust accountability regime. The IGIS further expressed a view that the current accountability arrangements 'are significant and effective'.[6]

[6] Inspector-General of Intelligence and Security, *IGIS submission to the Australian Law Reform Commission Review of Australian Privacy Law*, 6 December 2007, http://www.igis.gov.au/public_statements/submissions/IGIS_Submission_to_Review_of_Australian_Privacy_Law.pdf (7 March 2014)

Appendix 2: HOW ASIO SAFEGUARDS PERSONAL INFORMATION

ASIO takes very seriously its responsibility to protect and keep confidential any personal information it may hold about Australians, including persons under investigation as well as persons assisting ASIO to carry out its statutory responsibilities. The ASIO Act regulates the sharing of intelligence and ASIO has measures in place to secure and protect information it collects.

The following mechanisms seek to ensure that any access sought by ASIO of personal information is proportionate and that ASIO's use, handling and storage of personal information is managed in a manner that protects that information:

- ASIO has procedures in place to ensure the people of ASIO understand its legislation, internal policies and procedures and approach and accountability mechanisms
- ASIO's methods are required to be proportionate—and are in practice
- ASIO has detailed authorisation processes for establishing an investigation; and as the level of intrusiveness of proposed investigative activity increases so too does the seniority of ASIO officer required to authorise the activity
- ASIO's activities are subject to regular review by the IGIS, who reports on ASIO's compliance with laws and guidelines, propriety and adherence to human rights principles, to the Parliament, and
- ASIO's security intelligence activities are prioritised on the basis of greatest or most immediate threat or harm.

The Attorney-General's Guidelines to ASIO direct that, in undertaking investigations, there should be as little intrusion into individual privacy as possible. ASIO is also required to protect personal information from unnecessary or unauthorised public disclosure. The Guidelines direct ASIO in how to treat personal information:[7]

> **13 Treatment of Personal Information**
>
> 13.1 ASIO shall only collect, use, handle or disclose personal information for purposes connected with its statutory functions.
>
> 13.2 The Director-General shall take all reasonable steps to ensure that personal information shall not be collected, used, handled or disclosed by ASIO unless that collection, use, handling or disclosure is reasonably necessary for the performance of its statutory functions (or as otherwise authorised, or required, by law).
>
> 13.3 The Director-General shall ensure that all reasonable steps are taken to ensure that personal information held, used or disclosed by ASIO is accurate and not misleading.
>
> 13.4 Appropriate records shall be kept of all requests made by ASIO for access to personal information and all personal information received in response to such requests. Such records shall be open to inspection by the Inspector-General of Intelligence and Security.

[7] The Attorney-General's Guidelines can be accessed online at www.asio.gov.au/About-ASIO/Oversight-and-Accountability.html.

13.5 Appropriate records shall be kept of all communication by ASIO of personal information for purposes relevant to security or as otherwise authorised. Such records shall be open to inspection by the Inspector-General of Intelligence and Security.

13.6 The Director-General shall ensure that all personal information collected or held by ASIO is protected by reasonable security measures against loss and unauthorised access, use or modification.

ASIO officers must collect information using means that are proportionate to the gravity of the threat and its likelihood. The Attorney-General's Guidelines state: [8]

Conduct of inquiries and investigations

10.4 Information is to be obtained by ASIO in a lawful, timely and efficient way, and in accordance with the following:

(a) any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence;

(b) inquiries and investigations into individuals and groups should be undertaken:

(i) using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions; and

(ii) with due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest;

(c) the more intrusive the investigative technique, the higher the level of officer that should be required to approve its use;

(d) wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques; and

(e) where a threat is assessed as likely to develop quickly, a greater degree of intrusion may be justified.

These principles apply to ASIO's requests for access to personal information, and are reflected in ASIO's policies, procedures, and internal governance applying to investigative activities. Compliance with the Guidelines is overseen by the IGIS.

[8] The Attorney-General's Guidelines can be accessed online at www.asio.gov.au/About-ASIO/Oversight-and-Accountability.html.