UNCLASSIFIED

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

Review of the mandatory data retention regime

Submission to the Parliamentary Joint Committee on Intelligence and Security

The Hon Margaret Stone AO FAAL

Inspector-General of Intelligence and Security

2 August 2019

Table of Contents

1. Introduction

The Inspector-General of Intelligence and Security (IGIS) welcomes the opportunity to make this submission to the review by the Parliamentary Joint Committee on Intelligence and Security (the Committee) of the mandatory data retention regime established under Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). Information about the role of the IGIS is at **Attachment A**.

Consistent with established practices, IGIS does not make any comment on the policy underlying the provisions. IGIS makes a number of observations in the context of the office's role of overseeing and reviewing the activities of the intelligence agencies for legality and propriety and for consistency with human rights.

The mandatory data retention regime established by Part 5-1A of the TIA Act requires telecommunications service providers to retain prescribed data for a period of at least two years.[1] IGIS does not oversee these private sector service providers or the data retained by them. However, ASIO's access to retained telecommunications data, including under Chapter 4 of the TIA Act, does fall within the IGIS remit. IGIS understands that access to retained data by agencies, including ASIO, is within the scope of the Committee's current review.[2]

The Committee has indicated that it will focus its inquiry on the following aspects of the legislation:

- the continued effectiveness of the scheme, taking into account changes in the use of technology since the passage of the Bill;
- the appropriateness of the dataset and retention period;
- costs, including ongoing costs borne by service providers for compliance with the regime;
- any potential improvements to oversight, including in relation to journalist information warrants;
- any regulations and determinations made under the regime;
- the number of complaints about the scheme to relevant bodies, including the Commonwealth Ombudsman and the Inspector-General of Intelligence and Security;
- security requirements in relation to data stored under the regime, including in relation to data stored offshore;
- any access by agencies to retained telecommunications data outside the TIA Act framework, such as under the *Telecommunications Act 1997*; and
- developments in international jurisdictions since the passage of the Bill.

This submission makes comments in relation to the number of complaints made to IGIS; potential improvements to oversight, including in relation to journalist information warrants; and any access by agencies to retained telecommunications data outside the TIA Act framework.

[1] The prescribed data that is required to be retained by service providers is set out in section 187AA of the TIA Act.

[2] Section 187N of the TIA Act requires the Committee to review the operation of Part 5-1A of the TIA Act. Subsection (4) further requires the Director-General of Security to keep specified information relating to ASIO's access to telecommunications data under Division 3 of Part 4-1 of the TIA Act until the Committee's review is completed. As such, the 'operation of' Part 5-1A appears to be intended to extend to access to retained data by ASIO under Division 3 of Part 4-1.

2. Summary of submission

The following key points are raised in this submission:

- The Committee may wish to consider whether the current threshold for ASIO to access telecommunications data is appropriate. Noting the vast increase in data available (both quantitatively and qualitatively) since the current threshold was introduced more than ten years ago, the Committee may wish to consider whether existing requirements provide for adequate consideration of individual privacy.
- It may be appropriate for there to be a legislative requirement for the relevant ASIO officer to record, in each instance, the reasons for which an authorisation was given under Chapter 4 of the TIA Act.
- More generally, the Committee may wish to consider whether reporting requirements in relation to authorisations under Chapter 4 of the TIA Act should be strengthened, or whether reporting on data accessed outside the Chapter 4 framework, if any, should be required.
- IGIS supports the ASIO Guidelines being reviewed and re-issued, in consultation with this office, as a matter of priority. The Committee may wish to seek an update on the revision of the ASIO Guidelines, consistent with its 2014 and 2015 recommendations.
- There have been no changes to ASIO's legislation or policies since the introduction of the mandatory data retention regime that would require data that is not relevant, or no longer relevant, to security to be destroyed by ASIO. As such, IGIS considers this matter remains unresolved.
- The Committee may wish to consider whether it would be desirable to mandate some public reporting mechanisms in relation to journalist information warrants, in addition to ASIO's classified annual reporting. Agencies are best placed to advise the Committee of how, if at all, annual statistical reporting of warrant numbers may prejudice a particular operation.
- It may be appropriate for ASIO to be required to provide a report to the Attorney-General on each journalist information warrant that is issued, consistent with other types of warrants issued under the ASIO Act and TIA Act.
- The Committee may wish to discuss with relevant agencies the extent, if any, to which telecommunications data is accessed outside the framework provided by Chapter 4 of the TIA Act.

3. Background

3.1 ASIO access to retained data – Chapter 4 of the TIA Act

ASIO can access data available under the mandatory data retention regime (the regime) under the authorisation scheme set out in Chapter 4 of the TIA Act.

Chapter 4 was added to the TIA Act in September 2007 following the passage of the *Telecommunications (Interception and Access) Amendment Act 2007*, which implemented recommendations from the *Report on the Review of the Regulation of Access to Communications* by Anthony Blunn AO. The Act was intended to 'provide comprehensive and overriding legislation that regulates access to telecommunications data for national security and law enforcement purposes'.[3]

The *Telecommunications Act 1997* prohibits telecommunications carriers and carriage service providers from disclosing documents or information retained under the regime, insofar as the information or documents relate to:

- the contents or substance of a communication;
- carriage services supplied by the carrier; and
- the 'affairs or personal particulars' of a person (including mobile handset location data).[4]

Chapter 4 of the TIA Act provides exceptions to the general prohibition, enabling telecommunications data—other than the contents or substance of a communication[5]—to be disclosed to ASIO pursuant to section 175 or 176 of the TIA Act.[6] Section 175 enables 'eligible persons' within ASIO to authorise the carrier or carriage service provider's to disclose existing telecommunications data. Unlike a warrant, ASIO does not require ministerial approval to access this information. Instead, the Director-General, or any ASIO employee or ASIO affiliate approved by the Director-General as an 'eligible person', may authorise a carrier or carriage service provider to disclose existing information. The legislation does not specify the seniority of a person who may be approved to authorise the disclosure.

If a purpose of an authorisation is to identify a journalist's source, ASIO must first obtain a journalist information warrant under section 180G of the TIA Act.

It should be noted that although the prohibition in the *Telecommunications Act 1997* prevents carriers and carriage service providers from disclosing telecommunications data without a warrant or authorisation in place, it does not prevent agencies from accessing that data using other means.

---

[3] Parliament of the Commonwealth of Australia, House of Representatives, *Telecommunications (Interception and Access) Amendment Bill 2007: Replacement Explanatory Memorandum*, p. 1 [paragraph 2].

[4] *Telecommunications Act 1997*, ss 276 and 275A.

[5] TIA Act, s 172.

[6] Section 175 of the TIA Act permits the disclosure of existing data, whilst s 176 permits carriers and carriage service providers to provide ASIO with existing, and prospective telecommunications data (being data created after the time of the authorisation).

Threshold for access to retained data

ASIO may issue an authorisation to a carrier or carriage service provider wherever the eligible person granting the authorisation 'is satisfied that the disclosure would be in connection with the performance by the Organisation of its functions'.[7] As the former Inspector-General noted in a previous submission to the Committee, this is a low threshold.[8]

The current threshold was introduced more than ten years ago, when the volume and nature of communications data held by carriers and carriage service providers was quite different. IGIS notes the profound changes to the nature of telecommunications over the past decade, and expectations that the volume and types of telecommunications data held by carriers and carriage service providers will continue to grow.

ASIO's functions are set out in section 17 of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act). Broadly, the Organisation's functions are to obtain, correlate, evaluate and communicate intelligence relevant to security;[9] to undertake security assessments for Commonwealth and State purposes; to obtain foreign intelligence within Australia and to cooperate with certain other bodies. Given these broad functions, a range of requests for data held by carriers by virtue of the regime could be seen to be 'in connection with the performance of' those functions, whether or not the user of the service is suspected of engaging in activities prejudicial to security or is otherwise a target of ASIO investigation.[10]

As outlined above, the TIA Act prescribes few barriers to ASIO's access to data retained under the regime. Consequently, the risk of non-compliance with statutory requirements is low. However, supplementary guidance is provided by the *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)* (the ASIO Guidelines), which require that:

---

[7] TIA Act, s 175.

[8] IGIS Submission to the Parliamentary Joint Committee on Intelligence and Security review of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, *Submission 131*, 21 January 2015, p. 3.

[9] Section 4 of the ASIO Act provides that 'security' means:

(a) the protection of, and of the people of, the Commonwealth and the several 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
  (vi) acts of foreign interference;

whether directed from, or committed within, Australia or not; and

(aa) the protection of Australia's territorial and border integrity from serious threats; and

(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).

[10] This contrasts with the threshold for warrants under Part 2-2 of the TIA Act, which requires that the service in question has some connection to activities prejudicial to security, or particular classes of foreign intelligence.

- ASIO investigative activities should be undertaken using as little intrusion into individual privacy as is possible;[11]
- wherever possible the least intrusive techniques of information collection should be used before more intrusive techniques;[12]
- ASIO shall only collect, use, handle or disclose personal information for purposes connected with its statutory functions; and that
- all reasonable steps should be taken to ensure 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]

The ASIO Guidelines do not provide any guidance on what particular techniques are considered more intrusive than others.

The ASIO Guidelines are issued under subsections 8A(1) and 8A(2) of the ASIO Act. Although IGIS has been party to discussions with relevant departments and agencies about proposed revisions to the ASIO Guidelines for a number of years, the Guidelines were last updated over a decade ago (in late 2007). The proposed revision of the ASIO Guidelines is discussed in Part 5.4 of this submission.

3.2 IGIS inspections

ASIO authorisations for access

IGIS performs periodic inspections of ASIO's investigative cases, on a sampling basis. As part of these inspections, IGIS staff review telecommunications data authorisations issued by ASIO. These reviews may examine whether:

- the ASIO employee or ASIO affiliate who authorised the disclosure was approved by the Director-General to do so;[14]
- the collection of the information was in connection with the performance of ASIO's functions;[15] and
- whether the authorisation was consistent with the ASIO Guidelines.[16]

[11] ASIO Guidelines, cl 10.4(b)(i).

[12] ASIO Guidelines, cl 10.4(b)(d).

[13] ASIO Guidelines, cl 13.1 and 13.2.

[14] As required by s 175(2)(c) and (4) of the TIA Act.

[15] As required by s 175(3) of the TIA Act.

[16] As required by s 8A of the ASIO Act.

In these inspections IGIS finds a high level of compliance with the requirements of sections 175 and 176 of the TIA Act. This is not surprising given the low threshold for issuing such authorisations.[17]

ASIO handling and retention of data

In addition to IGIS's inspection of data authorisations, ASIO also informs IGIS where issues arise. For example, where a carrier erroneously provides information relating to a service other than the service specified in the ASIO authorisation. These circumstances are outside of ASIO's control (and IGIS jurisdiction). However, IGIS conducts an annual inspection of ASIO's information systems to ensure that where such errors are known to have occurred, the material is removed from ASIO's systems. These inspections form part of IGIS's broader program of reviewing the intelligence agencies' access to, handling and retention of personal information.

The ASIO Guidelines require that ASIO ensure personal information is not collected, used, handled or disclosed by ASIO other than for purposes connected with its statutory functions.[18] IGIS has identified occasional issues with ASIO's handling and retention of sensitive financial information and telecommunications data.[19] The 2017-2018 IGIS annual report noted:

> IGIS staff identified a small number of instances in which ASIO retained metadata, or telecommunications interception data that was not relevant to security. In one case ASIO intercepted a telecommunications service for two months before realising that the service was not used by ASIO's investigative target. ASIO ceased interception, but did not delete the data for over a year. The office raised concerns that the significant period taken to delete the data indicated deficiencies in ASIO's internal processes.[20]

IGIS is currently in the process of finalising its 2018–19 annual report. IGIS can provide further information about our inspection of ASIO's telecommunications data holdings following the release of that report.

4. Complaints to IGIS

IGIS does not receive complaints concerning the retention of telecommunications data by service providers under the data retention regime, which is outside this office's jurisdiction.

IGIS could consider any complaints received from service providers, employees or members of the public concerning ASIO's access to, use of or sharing of data retained under the scheme. No such complaints have been received in the period since the introduction of the mandatory data retention regime.

[17] IGIS Annual Report 2017-18, p. 22; IGIS Annual Report 2016-2017 p. 18.

[18] ASIO Guidelines, cl 13.1.

[19] IGIS Annual Report 2017-2018, p. 43.

[20] IGIS Annual Report 2017-18, p. 22.

It should be noted, however, that as ASIO's exercise of these powers is covert, the subjects of ASIO's requests, and persons whose telecommunications data is incidentally collected, are not usually aware that their telecommunications data has been accessed.

5. Potential strengthening of oversight

5.1 Threshold for authorisation

ASIO has previously informed the Committee about the critical importance of telecommunications data to its investigations in a changing technological and security environment.[21] Against this background, IGIS notes that the volume and nature of telecommunications data held by carriers and carriage service providers has continued to grow.

The threshold in section 175 of the TIA Act requires only that the ASIO officer issuing the authorisation is 'satisfied that the disclosure would be in connection with the performance by the Organisation of its functions'.[22] This is a substantially lower threshold than the threshold for ASIO to intercept telecommunications or access stored communications under a telecommunications service warrant issued under Part 2-2 of the TIA Act.[23] As noted earlier, the current threshold was introduced more than ten years ago, when the volume and nature of communications data held by carriers and carriage service providers was quite different.

IGIS notes that while section 187AA of the TIA Act mandates the minimum data set for retention, carriers and carriage service providers may choose to retain a broader array of telecommunications

---

[21] ASIO Submission to the Parliamentary Joint Committee on Intelligence and Security review of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, *Submission 12.1*, pp. 8, 19–20, 27.

[22] TIA Act, s 175.

[23] Section 9 of the TIA Act requires the Attorney-General to be satisfied of the following matters before issuing a Part 2-2 warrant, authorising the interception of a communication by ASIO:

> (a) the telecommunications service is being or is likely to be:
>
> > (i) used by a person engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, activities prejudicial to security; or
> >
> > (ia) the means by which a person receives or sends a communication from or to another person who is engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, such activities; or
> >
> > (ii) used for purposes prejudicial to security; and
>
> (b) the interception by the Organisation of communications made to or from the telecommunications service will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relating to security.

Part 3-2 of the TIA Act provides that, in addition to authorising interception of communications, a Part 2-2 warrant also authorises ASIO to access a stored communication.

information, which would be available to ASIO under section 175 and subsection 176(3) of the TIA Act (other than the 'contents or substance' of a communication).[24]

IGIS further notes that, unlike enforcement agencies, there is no requirement in the TIA Act for ASIO to consider privacy before making a Chapter 4 authorisation. In contrast, the authorised officer of an enforcement agency must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use of information is justifiable and proportionate, having regard to certain specified matters.[25] In its 2015 report, the Committee commented that a 'similar requirement should apply in respect of authorisations made by ASIO officers', and that this could be achieved by appropriate amendments to the ASIO Guidelines.[26] The existing ASIO Guidelines do require some consideration of individual privacy, as summarised earlier in this submission, but these requirements are not as strong as the requirements for enforcement agencies. As discussed below in Part 5.4, the ASIO Guidelines have not been updated since 2007.

IGIS suggests that the agencies are well positioned to outline the types and volume of data provided in response to agency requests, the number of requests, the level of authorising officers, and the extent, if any, to which disclosed data exceeds the minimum data set and retention period mandated by section 187AA of the TIA Act. IGIS suggests this insight would assist the Committee in assessing the regime's impact on privacy, and whether the current authorisation and oversight scheme is sufficient to protect these interests.

Threshold for authorisation

The Committee may wish to consider whether the current threshold for ASIO to access telecommunications data is appropriate. Noting the vast increase in data available (both quantitatively and qualitatively) since the current threshold was introduced more than ten years ago, the Committee may wish to consider whether existing requirements provide for adequate consideration of individual privacy.

In considering these matters, the Committee may wish to seek the advice of agencies on the types and volume of data provided in response to agency requests, the number of requests, the level of authorising officers, and the extent, if any, to which disclosed data exceeds the minimum data set and retention period mandated by section 187AA of the TIA Act.

5.2 Recording of reasons for authorisations

Section 175 enables the Director-General to approve any ASIO employee or affiliate, even a very junior officer, to authorise the disclosure of existing telecommunications data. This differs from section 176 of the TIA Act (authorisations for access to prospective information or documents), which allows only ASIO officers acting in a position equivalent to an SES Band 2 position to authorise disclosure.

[24] TIA Act, s 172.

[25] TIA Act, s 180F.

[26] Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 251.

The legislation does not require ASIO to record reasons for issuing a section 175 or section 176 authorisation, specific to the individual case, at the time that an authorisation is issued. Noting the wide range of ASIO employees and ASIO affiliates who may be approved to authorise the disclosure of telecommunications data, a legislative requirement for the relevant officer to record, in each instance, the reasons for which an authorisation was given would assist IGIS to provide assurance to Ministers, Parliament and the public that ASIO's access to this data is proportionate and proper.

Recording of reasons for authorisations

The Committee may wish to consider whether it would be appropriate for there to be a legislative requirement for the relevant ASIO officer to record, in each instance, the reasons for which an authorisation was given under Chapter 4 of the TIA Act.

5.3 Reporting requirements

ASIO is not required to publicly report on its access to telecommunications data. While annual reporting requirements require ASIO to report retrospectively on the number of authorisations issued under sections 175 and 176(3) in the previous year, and 'the purposes for which those authorisations were made',[27] these figures are only included in a classified appendix to ASIO's annual report.

Further, ASIO is not required to apply or report to Ministers on individual data access authorisations under Chapter 4 of the TIA Act. This differs from warranted intrusions into personal privacy such as the interception of telecommunications, interception of mail, search activities, or computer access activities.[28]

The Committee may wish to consider whether reporting requirements should be strengthened, or whether reporting on data accessed outside the Chapter 4 framework, if any, should be required. This could be achieved, for example, by enhancing the existing annual reporting requirements and/or by requiring periodic (for example, six-monthly) reports to the Minister on ASIO's access to telecommunications data during the preceding period.

Strengthening of reporting requirements

The Committee may wish to consider whether reporting requirements in relation to authorisations under Chapter 4 of the TIA Act should be strengthened, or whether reporting on data accessed outside the Chapter 4 framework, if any, should be required.

[27] ASIO Act s 94(2A)(c)–(d).

[28] TIA Act s 17, ASIO Act s 34.

5.4 The Attorney-General's Guidelines to ASIO

ASIO is exempt from the *Privacy Act 1988* and is not subject to the requirements of the Australian Privacy Principles.[29] As such, the ASIO Guidelines provide ASIO's key guidance regarding access to and handling of personal data.

The ASIO Guidelines were issued in late 2007, many years before the institution of this regime, or the widespread adoption of smartphone technology. Since the ASIO Guidelines were issued, ASIO has gained access to a range of intrusive powers, and has exercised these powers in a changing security and technological environment.

IGIS is of the view that the ASIO Guidelines are at their most effective if they are dynamic and regularly reviewed. IGIS supports the ASIO Guidelines being reviewed and re-issued, in consultation with this office, as a matter of priority.

This office has been party to discussions with relevant departments and agencies concerning the revision of the ASIO Guidelines. However, this has not yet resulted in new guidelines being issued.

IGIS suggests that the question of the relative intrusiveness of access to the different types of telecommunications data available under the regime, and broader questions surrounding ASIO's access to and retention of personal information, should be examined as part of the review process. IGIS suggests that a range of other matters, outside the scope of the Committee's current inquiry, should form part of this review.

Revision of ASIO Guidelines

The Committee may wish to seek an update on the revision of the ASIO Guidelines, consistent with its 2014 and 2015 recommendations.[30] IGIS supports the ASIO Guidelines being reviewed and re-issued, in consultation with this office, as a matter of priority.

[29] *Privacy Act 1988* s 7(1)(a)(i)(B)and s (2)(a). Section 7(2)(s)(i) refers to Division 1 of Part I of Schedule 2 of the *Freedom of Information Act 1982*. The schedule nominates ASIO, along with ASIS, ASD, ONI and IGIS, as exempt agencies.

[30] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the National Security Legislation Amendment Bill (No. 1) 2014,* September 2018, p. 46 (Recommendation 4); Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 262 (Recommendation 28).

5.5 Destruction of data that is not relevant, or no longer relevant, to security

The IGIS has previously highlighted to the Committee concerns in relation to the absence of a legislative requirement for ASIO to delete telecommunications data that is no longer needed.[31]

Section 31 of the ASIO Act and section 14 of the TIA Act require ASIO to destroy records of material obtained *under a warrant* if the Director-General is satisfied that the records are not required for the purposes of the performance by the Organisation of its functions or exercise of its powers (although there is no legislative requirement for the Director-General to make such a decision). For data obtained under a Chapter 4 authorisation, in contrast, there is no such requirement.

The ASIO Guidelines provide that:

> 11.2 Where an inquiry or investigation concludes that a subject's activities are not, or are no longer, relevant to security, the records of that inquiry or investigation shall be destroyed under schedules agreed to between ASIO and the National Archives of Australia.

The agreement referred to in the ASIO Guidelines is a Records Authority which sets out what material is to be retained indefinitely as national archives and specifies the minimum time that other records are to be kept. The Records Authority allows ASIO to extend the minimum retention period where it considers there is an administrative need to do so. Under the Records Authority most records documenting security intelligence collection activities are required to be retained indefinitely. The retention period for some other records is shorter and so ASIO is permitted to destroy this material earlier. Although the Authority states that records should be destroyed at the end of the prescribed retention period, it does not oblige ASIO to destroy any records.[32]

The Committee may recall that, in its *Advisory Report on the National Security Legislation Amendment Bill (No. 1) 2014*, the Committee recommended the Government initiate a review of the ASIO Guidelines, including 'examining requirements to govern ASIO's management and destruction of information obtained on persons who are not relevant, or no longer relevant, to security matters'.[33] Further, in its *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill* 2014, the Committee recommended that the Attorney-General's Department oversee a review of the adequacy of existing destruction requirements that apply to documents or information

[31] See IGIS submissions to the Parliamentary Joint Committee on Intelligence and Security's review of the National Security Legislation Amendment Bill (No. 1) 2014, *Submission 4*, p. 9; *Submission 4.1*, p. 1; IGIS submission to the review of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, *Submission 131*, p. 7; and oral evidence from Dr Vivienne Thom, then Inspector-General, to the review of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, *Committee Hansard*, Canberra, 29 January 2015, pp. 37, 40. See also IGIS, *Annual Report 2009–10*, pp. 18–19.

[32] Records Authority 2012/00324244.

[33] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the National Security Legislation Amendment Bill (No. 1) 2014,* September 2018, p. 46 (Recommendation 4).

disclosed pursuant to an authorisation under Chapter 4 of the TIA Act and held by enforcement agencies and ASIO.[34] Both recommendations were accepted by the Government.

As noted above, the ASIO Guidelines have not been updated since 2007, and there have been no changes to ASIO's legislation or policies that would require data that is not relevant, or no longer relevant, to security to be destroyed. As such, IGIS considers this matter remains unresolved.

Data destruction requirements

There have been no changes to ASIO's legislation or policies since the introduction of the mandatory data retention regime that would require data that is not relevant, or no longer relevant, to security to be destroyed by ASIO. As such, IGIS considers this matter remains unresolved.

6. Oversight of journalist information warrants

Division 4C of Part 4-1 of the TIA Act requires ASIO to first obtain a 'journalist information warrant', before making any authorisation in relation to a journalist for which a purpose is identifying the journalist's source.[35] Journalist information warrants are issued by the Minister, on request of the Director-General of Security. The Minister must apply a 'public interest' test before issuing a warrant, having regard to certain specified matters, including any submissions made by a Public Interest Advocate. The Minister, may specify certain conditions or restrictions relating to making authorisations under the authority of the warrant.[36]

The Director-General of Security is required to give the IGIS, as soon practicable, a copy of any journalist information warrant issued to ASIO. The Director-General is also required, as soon as practicable after the expiry of a warrant, to give the Inspector-General a copy of any authorisations made under the authority of the warrant.[37]

6.1 ASIO compliance to date

ASIO advises that it regards the number of journalist information warrants, if any, that have been issued to ASIO as being classified. However, the 2016-2017 IGIS annual report noted:

> In the course of our regular inspections we have observed that ASIO staff are familiar with ASIO internal policies and procedures relating to journalist information warrants. In one case, ASIO mistakenly obtained call charge records for a telephone service belonging to a newspaper's classifieds service. The metadata was collected due to a typographical error and was subsequently deleted. ASIO's response to this mistaken collection of metadata demonstrated

[34] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, February 2015, p. 262 (Recommendation 28).

[35] TIA Act, s 180G.

[36] TIA Act, s 180L.

[37] TIA Act, s 185D.

> ASIO staff's awareness of the legal requirements for obtaining a journalist information warrant.[38]

Since this time, IGIS has not identified any failures to comply with the legislative requirements of the journalist information warrants scheme.

6.2 Potential strengthening of reporting requirements

The Committee may wish to consider whether it would be desirable to mandate some public reporting mechanisms, in addition to ASIO's classified annual reporting.[39] Agencies are best place to advise the Committee of how, if at all, annual statistical reporting of warrant numbers may prejudice a particular operation.

Additionally, the Committee may wish to consider whether it would be appropriate to require ASIO to provide a report to the Attorney-General on each journalist information warrant that is issued, consistent with other types of warrants issued under the ASIO Act and TIA Act.[40] Reporting requirements could require ASIO to advise whether the data enabled ASIO to identify the journalist's source(s), and whether the information was shared or will be shared with other domestic or foreign agencies.

Reporting on journalist information warrants

The Committee may wish to consider whether it would be desirable to mandate some public reporting mechanisms in relation to journalist information warrants, in addition to ASIO's classified annual reporting. Agencies are best place to advise the Committee on what prejudice there may be to operations arising from annual statistical reporting.

The Committee may wish to consider whether it would be appropriate for ASIO to be required to provide a report to the Attorney-General on each journalist information warrant that is issued, consistent with other types of warrants issued under the ASIO Act and TIA Act.

7. Access to retained data outside Chapter 4 of the TIA Act

The Committee has indicated that it intends to focus its review on 'any access by agencies to retained telecommunications data outside the TIA Act framework, such as under the *Telecommunications Act 1997*'.

IGIS notes that sections 276, 277 and 278 of the *Telecommunications Act 1997* place obligations on carriers, carriage service providers, telecommunications contractors and related personnel to protect the confidentiality of telecommunications information. The framework in Chapter 4 of the TIA Act provides exceptions to these obligations, enabling ASIO and enforcement agencies to authorise the

[38] IGIS annual report 2016-2017, p. 17.

[39] ASIO Act, s 94(2A)(h)-(i) requires ASIO's annual report to record the number of journalist information warrants and associated authorisations issued during the reporting period.

[40] ASIO Act s 34, TIA Act s 17.

disclosure of information (other than the 'contents or substance of a communication')[41]. IGIS is aware that the *Telecommunications Act 1997* provides a range of other exceptions to these obligations, including access to telecommunications information under a warrant (such as warrants issued to ASIO under Part 2-2 of the TIA Act) or as otherwise required by or authorised under law.[42]

It should also be noted that although the obligations in the *Telecommunications Act 1997* prevent carriers and carriage service providers from disclosing telecommunications data without a warrant or authorisation in place, these obligations do not prevent agencies from accessing that data using other means. Any access by an agency to telecommunications data that does not require disclosure by a carrier or carriage service provider would therefore not require a warrant or authorisation, unless it also involved accessing content or unauthorised access to a computer.

Access to telecommunications data outside Chapter 4 of the TIA Act

The Committee may wish to discuss with relevant agencies the extent, if any, to which telecommunications data is accessed outside the framework provided by Chapter 4 of the TIA Act.

[41] TIA Act, s 172.

[42] *Telecommunications Act 1997*, s 280.

Attachment A: Role of the Inspector-General of Intelligence and Security

The Inspector-General is an independent statutory officer who reviews the activities of the following agencies:

- Australian Security Intelligence Organisation (ASIO);
- Australian Secret Intelligence Service (ASIS);
- Australian Signals Directorate (ASD);
- Australian Geospatial-Intelligence Organisation (AGO);
- Defence Intelligence Organisation (DIO); and
- Office of National Intelligence (ONI).

The Office of the IGIS is part of the Attorney-General's portfolio, and was previously located in the Prime Minister's portfolio from its commencement on 1 February 1987 until 10 May 2018. The IGIS is not subject to direction from any Minister on how responsibilities under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) should be carried out.

The *IGIS Act* provides the legal basis for the IGIS to conduct inspections of the intelligence agencies and to conduct inquiries of the Inspector-General's own motion, at the request of a Minister, or in response to complaints. The overarching purpose of the IGIS's activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights. A significant proportion of the resources of the Office are directed towards ongoing inspection and monitoring activities, so as to identify issues, including about the governance and control frameworks within agencies, before there is a need for major remedial action.

The inspection role of the IGIS is complemented by an inquiry function. In undertaking inquiries, the IGIS has strong investigative powers, including the power to require any person to answer questions and produce relevant documents, take sworn evidence, and enter agency premises. IGIS inquiries are conducted in private because they almost invariably involve classified or sensitive information, and the methods by which it is collected. Conducting an inquiry is resource intensive but provides a rigorous way of examining a complaint or systemic matter within an agency. The Inspector-General also receives and investigates complaints and public interest disclosures about the intelligence agencies. These come from members of the public and from current and former agency staff.

In response to the recommendations of the *2017 Independent Intelligence Review*, the Government announced that, subject to the introduction and passage of legislation, the jurisdiction of the IGIS will be extended to include the intelligence functions of the Department of Home Affairs, Australian Federal Police, Australian Criminal Intelligence Commission and Australian Transaction Reports and Analysis Centre. Resources for the IGIS have been increased to allow the office to sustain a full time equivalent staff of 55 (by 2019-20).