Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Submission to the Parliamentary Joint Committee on Intelligence and Security

Dr Vivienne Thom
Inspector-General of Intelligence and Security

21 January 2015

Table of Contents

Executive summary

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) will require certain carriers and internet service providers to keep prescribed telecommunications data for two years. Access by ASIO to that data will continue to be under the current arrangements in the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

The Inspector-General of Intelligence and Security (IGIS) does not have a role in relation to data retained by carriers, but does have an interest in the information accessed and retained by ASIO. This submission makes some observations based on the inspection of ASIO's access to telecommunications data:

- The legal threshold set in the TIA Act for ASIO to access telecommunications data under an authorisation is that the disclosure of the data to ASIO be 'in connection with the performance by the Organisation of its functions'. This is a low threshold. ASIO compliance with this test is high; there is no evidence of ASIO requesting telecommunications data for purposes not related to the performance of an ASIO function.

- The proposed amendments set *minimum* data retention requirement for telecommunications providers. Telecommunication data which exceeds this minimum set may be retained by carriers for business, cost efficiency or other reasons. Any additional data retained will continue to be accessible by ASIO under an authorisation.

- The Attorney-General's Guidelines require that ASIO investigative activities should be undertaken using as little intrusion into individual privacy as is possible, and that wherever possible the least intrusive techniques of information collection should be used before more intrusive techniques. Access to telecommunications data, particularly historical data, has been considered to be less intrusive than many other investigative techniques. The question of the relative intrusiveness of access to different telecommunications data could be examined as part of the review of the Attorney-General's Guidelines recently recommended by the PJCIS and supported by the Government.

- Once ASIO has lawfully obtained telecommunications data from a carrier or carriage service provider there is no statutory requirement for ASIO to either delete the data or to make an active decision as to whether the material is, or continues to be, relevant to security. The Attorney-General's Guidelines and an agreement with the National Archives allow most intelligence collected by ASIO to be retained indefinitely.

- There are occasional errors with data access requests and warrants where the incorrect data is sent to ASIO. In most instances the error is made by the carrier, not by ASIO. Errors can arise because of human error (for example incorrect entry of a number) or because of technological issues. ASIO is diligent in notifying my office of such errors and takes appropriate action to remove incorrectly received material from its holdings.

- The *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act) provides sufficient authority for the IGIS to continue oversight of ASIO access to telecommunications data. ASIO records of telecommunications data access requests are good and IGIS staff generally have access to relevant ASIO systems.

Background

Role of the Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory officer who reviews the activities of the Australian intelligence agencies. Of these agencies only the Australian Security Intelligence Organisation (ASIO) has authority under the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to request that a carrier provide telecommunications data.

The IGIS is currently supported by 14 staff (expected to increase to 16 by the end of 2014-15 as a result of additional funding). The Office of the IGIS (OIGIS) is an agency for the purposes of the *Public Service Act 1999* and a non-corporate Commonwealth entity for the purpose of the *Public Governance, Performance and Accountability Act 2013.*

The Office of the IGIS is situated within the Prime Minister's portfolio. The IGIS is not subject to direction from the Prime Minister, or other ministers, on how responsibilities under the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act) should be carried out.

The IGIS Act provides the legal basis for the IGIS to conduct inspections of the intelligence agencies, to handle complaints and to conduct inquiries of the Inspector-General's own motion or at the request of a Minister.

The overarching purpose of IGIS's activities is to ensure that each intelligence agency acts legally and with propriety, complies with ministerial guidelines and directives, and is consistent with human rights. A significant proportion of the resources of the office has in the past been 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. OIGIS staff have access to all documents of the intelligence agencies and the IGIS is often proactively briefed about sensitive operations.

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 highly 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 particular complaint or systemic matter within an agency.

Telecommunications data requests reviewed as part of IGIS inspections

OIGIS staff regularly examine ASIO telecommunications data authorisations as part of the regular program of inspection of ASIO inquiries and investigations. During these inspections, OIGIS staff review the records of a selected sample of cases. The inspection team looks at records associated with activities that form part of the ASIO inquiry or investigation. This includes telecommunications data authorisations (historical and prospective), warrants, and any other activities that form part of the inquiry or investigation.

In relation to telecommunications data authorisations, the inspections examine:

- whether the authorisation was approved at the appropriate level, noting that approval for prospective data authorisations must be at a higher level than historical data authorisations
- whether the collection of that information is related to ASIO's functions

- whether there was compliance with the Attorney-General's Guidelines, in particular whether the activity was proportionate to the gravity of the threat, and whether there was sufficient justification for not using less intrusive methods to obtain the data.

ASIO access to telecommunications data

TIA Act — Access in connection with the performance of an ASIO function

Sections 175 and 176 of the TIA Act allow nominated ASIO employees and ASIO affiliates[1] to authorise a carrier or carriage service provider to disclose prospective and existing telecommunications data. The relevant ASIO employee or ASIO affiliate must not make the authorisation unless:

> he or she is satisfied that the disclosure would be *in connection with* the performance by the Organisation of its functions.

ASIO staff must also comply with Guidelines made by the Attorney-General under the ASIO Act in the performance of their functions.

ASIO's functions are set out in s17 of the *Australian Security Intelligence Organisation Act 1979* (the ASIO Act). Broadly, its functions are to obtain, correlate, evaluate and communicate intelligence relevant to security; to undertake security assessments for Commonwealth and State purposes; to obtain foreign intelligence within Australia and to cooperate with certain other bodies.

The test that ASIO is required to meet in order to obtain data under s175 and 176 is different to the test in the Act that law enforcement agencies are required to meet to obtain the same data which is that the disclosure is *reasonably necessary* for the enforcement of the criminal law.[2]

Requests for historical data can be made by an ASIO employee or an ASIO affiliate in a class approved by the Director-General of Security for this purpose. The level at which that delegation has been set is lower than that for prospective data requests.[3]

High level of ASIO compliance with TIA Act requirements

There is a consistently high level of compliance with the requirement that ASIO employees and affiliates only request telecommunications data in connection with an ASIO function. In my 2013-14 Annual Report I commented that:

> ASIO's access to prospective telecommunications data is reviewed as part of our regular inspection program. Due to their intrusive nature, access to prospective and historical telecommunications data are reviewed in a similar manner to telecommunications warrants.
>
> I did not identify any concerns with ASIO's access to prospective and historic telecommunications data. My office's oversight of this particular investigative technique decreased during this reporting period due primarily to changes in our inspection program and the high rate of compliance in this area.
>
> I am satisfied that prospective data authorisations reviewed were endorsed by an appropriate senior officer, and that ASIO has regard to the Attorney-General's Guidelines and is meeting the legislative requirement to only make requests for data in connection with the performance of its functions.[4]

[1] An 'ASIO affiliate' is a person performing functions or services for ASIO in accordance with a contract, agreement or other arrangement. Only ASIO affiliates covered by a specific approval can authorise the disclosure of historical telecommunications data.
[2] See sections 178-180 of the TIA Act
[3] For prospective data authorisations an SES level 2 or equivalent level officer is required to give the authorisation.

There are occasional errors with data access requests and warrants where the incorrect data is sent to ASIO. In most instances the error is made by the carrier, not by ASIO. Errors can arise because of human error (for example incorrect entry of a number) or because of technological issues. ASIO is diligent in notifying my office of such errors and takes appropriate action to remove incorrectly received material from its holdings.

If carriers retain more than minimum set, ASIO can access that data

The Bill, if enacted, would require entities that supply telecommunications services in Australia to retain prescribed telecommunications data for two years, subject to appropriate exemptions. How much, if any, data beyond the minimum each provider actually retains will be a matter for each provider based on their own business requirements and any technological and cost factors.

For example, the proposed mandatory data set includes limited location information – the location at the start and end of a communication. It is not clear whether it will be easy, or cost efficient, for carriers to filter information so that only this minimum is retained or whether they will find it easier to simply retain more comprehensive location information associated with a communication. It is possible that the answer to this will vary between carriers and might change over time.

If telecommunications suppliers do retain more than the minimum required then whatever information they retain, so long as it is not content, will be able to be accessed and retained by ASIO under an authorisation.

ASIO must also comply with the Attorney-General's Guidelines

ASIO is required to comply with Guidelines made by the Attorney-General under s8A of the ASIO Act. The current Guidelines require that:

> 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.

Access to telecommunications data, both historical and prospective, is an important and frequently used tool for ASIO. As a Deputy Director-General of Security stated in evidence to an earlier hearing of this Committee:

> Metadata is often used as our first point in an investigation. So we see it as the least intrusive stage. It is as much to rule people in as to rule people out of investigations so that we do not then need, in many cases, to go to another higher level of intrusion …[5]

[4] IGIS Annual Report 2013-14 p21
[5] PJCIS Hansard Wednesday 17 December 2014 p17

In my view, not all requests for access to telecommunications data should be treated as being of equal weight in terms of invasion of privacy. Some requests are for a single piece of information; others potentially cover a significant amount of information which could reveal a lot about an individual's relationships, beliefs and location. The changes proposed by the Bill will mean that, as a minimum, ASIO will have access to two years of prescribed data with each request. As noted above some providers may retain information beyond the minimum required and this will continue to be able to be accessed by ASIO with an authorisation (provided it is not content, which would require a warrant).

Our inspections of ASIO investigations confirm that ASIO has regard to the Guidelines. The PJCIS recently recommended a review of the Guidelines and the Government announced it would request ASIO and the Attorney-General's Department to undertake a review of the Guidelines, including examining requirements to govern ASIO's management and destruction of information obtained on persons who are not relevant, or are no longer relevant, to security matters.[6] The Committee may like to consider whether that review should also look at the relative intrusiveness of different types of data requests, particularly in light of any changes made by the Bill.

Telecommunications data obtained by ASIO may be retained indefinitely

There is no requirement in the TIA Act, the ASIO Act or in the Bill that would require ASIO to destroy telecommunications data it has obtained from a carrier after a certain period of time, nor is there any legislative requirement for ASIO to make an active decision as to whether telecommunications data (or other material) is not relevant or is no longer relevant to security and to destroy that material.

The only legislative provisions that deal directly with destruction of telecommunications related information are s31 of the ASIO Act and s14 of the TIA Act. These require that ASIO destroy records of material *obtained under a warrant* if the Director-General is satisfied that the records are not required for the purpose of the performance of its functions. I have recently been advised by ASIO that the power had not been delegated and that the Director-General does not currently make any decisions under these provisions. Therefore currently no records are destroyed under these provisions. In any event it should also be noted that these provisions do not apply to telecommunications data obtained under an authorisation.

There is no doubt that telecommunication data forms an important part of ASIO investigations into security matters. It is reasonable for data that is relevant to an ongoing operation to be retained. Some operations run for many years. However if data that is obtained 'in connection with an ASIO function' turns out to be not relevant to security or is relevant but only for a period of time, there is no positive requirement for ASIO to delete this data. This is a privacy issue that needs to be balanced against the need for ASIO to obtain and analyse data in order to identify material relevant to security.

The Attorney-General's Guidelines provide guidance on what 'relevant to security' means. It includes material that assists in determining whether the activities of a subject are *not* relevant to security. The Guidelines also explicitly allow ASIO to maintain a broad database of reference material.[7]

[6] Recommendation 4 of the *Advisory Report on the National Security Legislation Amendment Bill (No.1) 2014*, Parliamentary Joint Committee on Intelligence and Security, September 2014. Government response at http://www.attorneygeneral.gov.au/Mediareleases/Documents/ResponsePJCISreportNSLAB.pdf

[7] See guideline 10.1 on 'relevant to security' and guideline 6.2 on maintaining a comprehensive body of reference material.

The 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 with Archives' is a Records Authority which sets 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.[8] The retention period for some other records is shorter and so ASIO is *permitted* to destroy this material earlier.[9] 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.[10]

The issue of how long ASIO keeps data that it has obtained from telecommunications carriers and other sources is one that the IGIS office has commented on before. For example in relation to the retention of data by ASIO, the 2009-10 IGIS annual report noted:

> Our interest in ASIO's retention and destruction of data arises from the Attorney–General's Guidelines which were issued to ASIO by the then Attorney–General, the Hon. Philip Ruddock MP, in October 2007 (the 2007 Guidelines). These guidelines replaced earlier guidance issued by the then Attorney–General, the Hon. Michael Duffy MP, in December 1992 (the 1992 Guidelines).
>
> Around the time that the 2007 Guidelines were issued, [the then IGIS] commented that while he was supportive of many of the changes, the office would take a close interest in ASIO's information management governance framework, with a particular focus on what data ASIO retains or destroys in future inspections.
>
> This is a difficult issue because the real significance of some (but not all) data may only become apparent when it is correlated with other data which becomes available subsequently. At the same time, ASIO is required to comply with Ministerial Guidelines which preclude ASIO from retaining high volumes of data, including significant data holdings which prove to have no relevance to organisational objectives.
>
> The 1992 Guidelines contained an express prohibition on so–called 'speculative data matching' which does not appear in the 2007 Guidelines. Instead, the 2007 Guidelines are more permissive as to what data ASIO may collect, including as 'reference' data, although this is subject to the general limitation that material be 'relevant to security'.
>
> Data sets are only one element of the information which ASIO collects. In relation to other material there is also the question of what should be done with individual records over time, particularly data which proves not to be, or to no longer be, relevant to security.

The Archives Record Authority commenced in September 2012. ASIO record retention practices have been identified as an area for IGIS inspection in 2015.

---

[8] See class 61098. This class of records includes 'field inquiries, investigations, telecommunications interception and operational activities'. It also includes 'investigations of individuals, groups and organisations no longer of security interest.'

[9] For example Class 61101 allows 'routine' security intelligence collection to be destroyed after 20 years. Class 61103 allows material *not* covered by 61098-61102 including investigations of individuals identified as not of security interest and…data…acquired…and identified as not of security interest for ongoing investigations, internal reference or litigation purposes' to be destroyed after 5 years.

[10] Records Authority 2012/00324244

The Committee may like to consider whether the Records Authority should be reviewed and whether the review of the Attorney-General's Guidelines mentioned above should also look at whether additional guidance to ASIO about access to, or retention of, telecommunications data needs to be included in view of any changes made by the Bill.