Submission by the Commonwealth Ombudsman

Review of the mandatory data retention scheme

Submission by the Commonwealth Ombudsman, Michael Manthorpe

July 2019

Contents

Introduction

The Office of the Commonwealth Ombudsman welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (the Committee) in response to its review of the mandatory data retention scheme.

The purpose of the Office of the Commonwealth Ombudsman (the Office) is to:

- provide assurance that the organisations we oversight act with integrity and treat people fairly, and
- influence systemic improvement in public administration in Australia and the region.

We seek to achieve our purpose through:

- correcting administrative deficiencies through independent review of complaints about Australian Government administrative action
- fostering good public administration that is accountable, lawful, fair, transparent and responsive
- assisting people to resolve complaints about government administrative action; and
- providing assurance that Commonwealth, State and Territory law enforcement, integrity and regulatory agencies are complying with statutory requirements and have sound administrative practices in relation to certain covert, intrusive and coercive powers.

Of particular relevance to the Committee's review is the Office's role under Chapter 4A of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to oversee 20 criminal law enforcement agencies' use of the telecommunications data powers under Chapter 4 of the TIA Act (i.e. the mandatory data retention scheme).

Under Chapter 4A, the Office is required to determine the extent of compliance by an agency and its officers with legislative requirements. We achieve this by conducting on-site inspections of agencies' records.[1] The Ombudsman must report annually to the responsible Minister (the Minister for Home Affairs) on the outcome of those inspections.

Response to Terms of Reference

To assist the Committee in its review, this submission addresses the following Terms of Reference relevant to the Office's role:

- the continued effectiveness of the scheme
- any access by agencies to retained telecommunications data outside the TIA Act framework
- any regulations and determinations made under the scheme
- the number of complaints about the scheme, and
- any potential improvements to oversight, including in relation to journalist information warrants.

[1] This process does not involve assessing the merits of an agency's decision to exercise the telecommunications data powers.

We have identified a number of issues affecting agency compliance and shortcomings within the legislation, which are detailed in the submission. However, we consider that agencies are generally committed to using the scheme in a manner that complies with statutory requirements and is consistent with the 'spirit' of the legislation. Agencies are receptive to our findings and suggestions for improvement and have continued to engage with our Office to clarify and disclose issues affecting their compliance with the scheme.

The continued effectiveness of the scheme

Based on our experience, we have made a number of observations regarding the effectiveness of the mandatory data retention scheme including potential gaps, ambiguities or inconsistencies in the legislation.

In our view, the following issues present challenges for the continued effectiveness of the scheme:

- the lack of a framework for agencies to verbally issue authorisations for access to telecommunications data, despite agencies adopting this practice in urgent or out-of-hours circumstances

- the absence of any obligation on agencies to retain the telecommunications data they receive from a carrier under an authorisation or any obligations regarding the destruction of that data, and

- ambiguity regarding what constitutes 'content' and whether agencies should have access to this information when disclosed by a carrier under an authorisation.

Lack of a framework for verbal authorisations

Chapter 4 of the TIA Act provides the legislative framework under which certain criminal law enforcement agencies may access telecommunications data for the purposes of enforcing the criminal law, locating a missing person or enforcing a law imposing a pecuniary penalty or protection of the public revenue.

An agency may access a person's telecommunications data by internally issuing a 'telecommunications data authorisation' (authorisation) that it then provides to a carrier for processing.[2] An authorisation can only be issued by an appropriately authorised member of an agency (referred to as an 'authorised officer')[3] and may authorise access to existing data a carrier holds (referred to as a 'historic authorisation')[4] or may require a carrier to retain data it receives in future (referred to as a 'prospective authorisation')[5]. In limited circumstances, an agency may have to obtain a journalist information warrant before it can internally issue an authorisation.[6] Only the Australian Federal Police (AFP) may issue an authorisation on behalf of a foreign law enforcement agency.[7]

Currently, there is no framework under the scheme to enable an agency to verbally issue an authorisation. In our 2016—17 Annual Report under s 186J of the TIA Act, we reported that a

[2] Except in relation to telecommunications data obtained from the Integrated Public Number Database (IPND) – agencies can access this system without carrier assistance.
[3] See TIA Act, s 5AB.
[4] Ibid, ss 178, 178A and 179.
[5] Ibid, s 180.
[6] Ibid, s 180Q.
[7] Ibid, ss 180A-D.

number of agencies had adopted a practice of verbally approving access to telecommunications data.[8] Typically, agencies adopt this practice where the circumstances of its investigation are considered urgent or the request is made 'out-of-hours' when key personnel, such as the agency's compliance area, are unable to assist in the handling of the request. In some instances the agency may prepare a written authorisation following the verbal approval, however sometimes no written record is made.

Verbal authorisations are not specifically provided for under the scheme.[9] The following provisions of the TIA Act also tend to suggest that verbal authorisations cannot be implied into the scheme:

- an authorisation can only be in written or electronic format (s 183(1)(e))
- an authorisation must comply with such requirements as are determined by the Communications Access Co-ordinator (CAC) (s 183(1)(f)). The CAC has issued requirements which specify that an authorisation, whether in written or electronic form, must be signed by its maker (the authorised officer who issues it)[10]
- the chief officer of an agency must keep documents or other materials to indicate whether an authorisation was properly issued, including whether the authorised officer took into account all relevant matters (s 186A(1)(a)(i)), and
- an authorised officer must consider privacy before issuing an authorisation (s 180F).

We acknowledge there are operational circumstances including urgency that may mean a verbal authorisation would be of assistance to law enforcement agencies. However, this should be supported by legislative provision.[11]

The Committee may wish to consider whether the scheme should be amended to provide a framework for agencies to verbally approve authorisations in limited circumstances, such as urgency. Such amendment should include appropriate record keeping obligations.

No framework for the destruction of telecommunications data

Currently, there is no framework under the scheme for the destruction of telecommunications data obtained by an agency. The lack of a statutory framework to manage agencies' destruction of telecommunications data means an agency can destroy the data it obtains under an authorisation at its own discretion. There are no provisions requiring the agency to keep records of when such information is destroyed or who authorised the destruction.

[8] See 'A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979* – for the period 1 July 2016 to 30 June 2017', pg 16 http://www.ombudsman.gov.au/__data/assets/pdf_file/0033/96747/201617-Chapter-4A-Annual-Report.pdf

[9] This is in direct contrast to s 40(2) of the TIA Act which specifically provides for telephone applications for telecommunications interception warrants in urgent circumstances.

[10] See *Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2018*, Part 2, Division 1.

[11] Examples of mechanisms for agencies to expedite approval process in urgent circumstances in other legislation we oversee include: *Crimes Act 1914*, Part IAB, ss 15GH(2)(b) and 15GJ(1)(b) (urgent applications and authorities for controlled operations); *Surveillance Devices Act 2004*, Part 3 (emergency authorisations); TIA Act, ss 40(2)(b), 43 and 46(1)(b) (urgent applications for telecommunications interception warrants) and ss 111(2)(b), 114 and 116(1)(b) (urgent applications for stored communications warrants).

In this way, the scheme differs from other legislation we oversee relating to the use of covert powers by law enforcement which place statutory requirements on agencies when destroying such information and we assess those destructions.[12]

The Office does not draw a negative inference from the destruction of telecommunications data by an agency as we are mindful information may be destroyed for many reasons, including where it is no longer considered relevant to an investigation. We also note the potential practical challenges of placing destruction obligations on agencies given the volume of use of the scheme. However, in the absence of such a framework there is no oversight of how agencies destroy telecommunications data.

The Committee may wish to consider whether there is a need for the establishment of a framework to manage agencies' destruction of telecommunications data.

No requirement to retain telecommunications data for an Ombudsman inspection

When overseeing the use of covert powers we assess whether the information obtained by an agency complies with the instrument (i.e. the authorisation or warrant) which provides the authority for use of the power. This is a fundamental check, particularly from a public interest perspective, as it assesses whether an agency has acted in accordance with the authority provided to them.

In relation to the mandatory data retention scheme, we assess the telecommunications data provided by the carrier to the agency against the parameters set by the relevant authorisation. In instances that carriers provide data outside those parameters, we acknowledge that is the carrier's error; however, it is still incumbent on agencies to check all the data they receive is authorised. Where we identify information that is outside of the authorisation, we notify the agency and suggest it:

- quarantine that information from any further use, and
- where relevant, seek legal advice on any use made of the information to date.

We follow up at our next inspection to confirm what, if any, remedial action the agency has taken.

There is no requirement under the TIA Act for agencies to retain the telecommunications data they receive from a carrier for a particular period or for the purposes of an inspection. Although s 186A(3) of the TIA Act mandates that agencies keep certain records for a period of three years or until we have reported to the Minister under s 186J, these obligations do not include a requirement to retain the telecommunications data obtained under an authorisation.

In the majority of instances agencies have retained the telecommunications data and we have been able to inspect the data against the authorisation. However, in some instances agencies have destroyed telecommunications data obtained under an authorisation by the time of our inspection. In these instances, because the information has already been destroyed, we are unable to check whether the telecommunications data the agency received complied with the parameters set by the relevant authorisation.

[12] See for example, *Surveillance Devices Act 2004*, ss 46, 46A and 52(1)(j) (surveillance devices), TIA Act ss 79, 79AA, 79A and 81(1)(d)(iii) (telecommunications interceptions) and ss 150 and 151(1)(i) (stored communications).

The Committee may wish to consider whether there is a need for the record-keeping requirements under s 186A(1) of the TIA Act to be expanded to require agencies to retain telecommunications data for the purposes of an Ombudsman inspection.

Determining what constitutes 'content'

Under s 172 of the TIA Act, an authorisation does not permit the disclosure to an agency of information that is the content or substance of a communication, or a document that contains the content or substance of a communication. The term 'content or substance of a communication' is not defined in the TIA Act.

For the majority of telecommunications data we inspect, our Office is able to determine whether the disclosed information breaches the restriction in s 172. For example, the telecommunications data of a phone call can include the date, time and location(s) of the call but cannot include the substance of what the parties said.

For other data types, it has been difficult for our Office to make this determination. For example, we have identified instances where carriers have returned telecommunications data that has included a person's Internet Protocol (IP) address and the Uniform Resource Locators (URLs) they have searched. In other instances, carriers have provided account (i.e. subscriber) information to an agency which included account numbers and addresses recorded for the subscriber.

It is unclear whether such information breaches the restriction under s 172 and depends on a case-by-case assessment. Where we consider that information does amount to content, we notify the agency and suggest it:

- quarantine that information from any further use, and
- where relevant, seek legal advice on any use of the information to date.

We follow up at our next inspection to confirm what, if any, remedial action the agency has taken.

Clarity on what constitutes 'content' would likely assist:

- carriers in determining what information they can provide to agencies under an authorisation
- agencies in identifying when they may have received content from a carrier so that they can take immediate steps to limit any use of that information, and
- our Office in assessing whether the telecommunications data accessed by an agency complies with the restriction under s 172.

The Committee may wish to consider whether the Act should be amended to include a definition of the term '*content or substance of a communication or document*'.

Determining the time of revocation

Section 180(7) of the TIA Act states that an authorisation must be revoked if the authorised officer is satisfied that disclosure of the telecommunications data is no longer required. However, the legislation is silent as to when a revocation takes effect. This is an important consideration as it determines the point in time an authorisation ceases to be in force and, in turn, removes the basis upon which the agency can access the telecommunications data.

If the revocation instrument specifies the date and time it is to take effect, we will take this to be the point in time at which the authorisation is revoked and, therefore, no longer in force. In other

instances, our Office has relied upon agencies' policies and procedural documents to determine the time of effect. In some cases, compliance issues have arisen for agencies as a result of the unavoidable delay between the revocation instrument being signed and the agency notifying the carrier. In these circumstances, we have seen instances where a carrier continues to send telecommunications data to the agency post-revocation on the assumption that the authorisation remains in force. For this reason, some agencies have implemented a practice whereby the revocation instrument will specify that revocation takes effect after the carrier is notified.

The Committee may wish to consider whether the Act should be amended to specify when a revocation of an authorisation takes effect.

Access by agencies outside of the scheme

The Ombudsman does not have oversight of carriers or their actions in responding to requests for telecommunications data made outside of the mandatory data retention scheme.

During our inspections, we ask agencies whether they have sought access to telecommunications data under legislation other than the TIA Act. Agencies have typically been forthcoming in providing this information, which has revealed that some agencies have sought access to telecommunications data under the following legislation:

- *Telecommunications Act 1997*[13]
- *Migration Act 1958*,[14] and
- *Coroners Act 1995* (Tas).

While we are aware of this issue, it is beyond the scope of our role to examine agencies' access to telecommunications data outside of the TIA Act. As noted in our response to the Committee to Questions on Notice arising from the Ombudsman's 16 November 2018 appearance,[15] our Office is not aware of any external oversight of access to telecommunications data outside of the TIA Act.

While the Ombudsman could use his own motion powers under the *Ombudsman Act 1976* (the Ombudsman Act) to examine Commonwealth agencies' access to such information, there are several reasons why these general powers may not be well-suited to providing an effective or comprehensive oversight mechanism. For example:

- the absence of any notification or reporting obligations for agencies means our Office does not have clear visibility of if, or when agencies access telecommunications data outside an authorisation made under the TIA Act
- our Office does not have jurisdiction to examine State or Territory agencies' access to such information, and
- the Ombudsman Act provides powers for our Office to examine the actions and decisions of Commonwealth agencies. We do not have jurisdiction to investigate actions or decisions carriers may take in response.

[13] Specifically under ss 280(1)(b), 287 and 313.
[14] For example, under s 18.
[15] See Commonwealth Ombudsman, Questions on Notice from Public Hearing on 16 November 2018 (Submission: 64.2) https://www.aph.gov.au/DocumentStore.ashx?id=8ae24860-e741-450a-a500-17c0e3455379&subId=661188.

The Committee may wish to consider whether there should be external oversight of access to telecommunications data outside the TIA Act.

Complaints about the scheme

Under the Ombudsman Act, the Ombudsman can receive complaints about the actions of Australian Government agencies and certain prescribed private sector organisations. We may investigate the complaint if we consider those actions to be wrong, unjust, unlawful, discriminatory or unfair.

Under the mandatory data retention scheme, an agency's actions are covert so a person is typically unaware that an agency has accessed their telecommunications data. As a result, it is unlikely that the Office will receive a complaint about an agency's actions to access telecommunications data under the scheme. The Ombudsman's jurisdiction under the Ombudsman Act extends only to the actions of Commonwealth agencies (and certain prescribed private sector agencies), and the Office is unable to investigate complaints about the actions of State and Territory agencies. For these reasons, the Ombudsman has received only a small number of complaints about the scheme.

Since the commencement of the scheme on 13 October 2015, the Ombudsman has received two complaints relevant to the Committee's review. The first complaint (ref 2016-502150) alleged that a local council in NSW had accessed the complainant's telecommunications data. This complaint was outside of the Ombudsman's jurisdiction and the complainant was referred to the NSW Ombudsman.

The second complaint (ref 2017-505262) alleged 'abuse', generally, by the AFP of the mandatory data retention scheme. The Office referred the complainant to the Professional Standards Unit, the complaint handling area within the AFP.

Potential improvements to oversight

The Ombudsman has differing levels of oversight under the TIA Act. In the course of undertaking our oversight activities we have identified the following issues for the Committee's consideration:

- a potential limit to the application of the journalist information warrant provisions, and
- the need for broader reform of the TIA Act.

Potential limit to the application of journalist information warrant provisions

Under s 180H of the TIA Act, before an agency can internally issue an authorisation for the purpose of identifying a journalist's source, it must obtain a 'journalist information warrant'. This requirement under the mandatory data retention scheme is intended to balance the public interest in protecting journalists' sources with the need for agencies to access the investigative tools necessary to protect the community.

We highlighted in our October 2017 report on the AFP's compliance that there is a potential limit in the application of the legislation.[16] Where an agency seeks to access telecommunications data

[16] See 'A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the Telecommunications (Interception and Access) Act 1979 – Access to journalist's telecommunications data without a journalist information warrant', pgs. 3 and 8 http://www.ombudsman.gov.au/__data/assets/pdf_file/0021/78123/Commonwealth-Ombudsman-AFP-JIW-report-PDF-FOR-WEBSITE.pdf.

of a person (the source) but that person is neither a journalist nor a journalist's employer, the agency is not required to obtain a journalist information warrant to identify the person as a journalist's source.

This is because the current drafting of s 180H(1) applies a two-limb test to identify when a warrant is required:

> (1) An authorised officer of an enforcement agency must not make an authorisation that would authorise the disclosure of information or documents relating to a particular person if:
>
> a) the authorised officer knows or reasonably believes that particular person to be:
>
> i) a person who is working in a professional capacity as a journalist; or
>
> ii) an employer of such a person; and
>
> b) a purpose of making the authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source;
>
> unless a Journalist Information Warrant is in force, in relation to that particular person, under which authorised officers of the agency may make authorisations under that section.

If the first limb of this test is not satisfied – i.e. the person whose telecommunications data the agency is seeking to access is not working in a professional capacity as a journalist and is not the employer of such a person – the agency will not be required to obtain a warrant before issuing an authorisation and there will be no oversight by an external issuing authority or a Public Interest Advocate, despite the possibility that agencies have sought access to that telecommunications data for the purposes of confirming whether the person disclosed information to a journalist, and therefore whether they are a journalist's source.

The Committee may wish to consider whether the current drafting of s 180H unintentionally limits the application of journalist information warrant requirements.

Broader reform of the TIA Act

The Committee's review of the mandatory data retention scheme provides an opportunity to consider the need for broader reform of the TIA Act. While we appreciate that there may be a specific review of the TIA Act as a whole, we take this opportunity to raise the following issues with the Committee:

- the alignment of existing oversight frameworks
- inconsistencies in destruction requirements, and
- the retention of stored communications for the purposes of an Ombudsman inspection.

Alignment of existing oversight frameworks

Chapter 4A of the TIA Act provides a comprehensive oversight framework that requires our Office to inspect and publicly report on agencies' compliance when using the stored communications and telecommunications data powers under Chapters 3 and 4 of the TIA Act. The Office also has a role in overseeing Commonwealth agencies' use of the telecommunications interception powers under Chapter 2.

In our view, agencies' use of the telecommunications interception powers, which authorise the interception of a person's live communications, involves greater privacy intrusion than the accessing of their stored communications (such as SMS, MMS, voicemail and emails) and telecommunications data (i.e. the information about their communications). This is recognised

within the TIA Act by the higher thresholds placed on agencies' use of the telecommunications interception powers, including that they must be investigating a "serious offence", as defined in s 5D of the TIA Act, and obtain a warrant from an external issuing authority.

Despite this, the Ombudsman's oversight of Chapter 2 is comparatively narrower than that provided under Chapter 4A of the TIA Act. Under s 83, the Ombudsman's oversight of telecommunications interceptions is limited to assessing compliance by Commonwealth agencies only in relation to their record-keeping and destruction obligations.[17] Our Office does not provide a public report to the Minister under Chapter 2,[18] which we consider is critical to our ability to influence improvements in agency compliance and to provide assurance to the public and Parliament on the use of the powers.[19]

To increase accountability and transparency by agencies when conducting telecommunications interception, the Office would welcome the alignment of the oversight framework under Chapter 2 with the comprehensive model provided for by Chapter 4A of the TIA Act.

Inconsistencies in destruction requirements

As previously stated, there is currently no framework under the scheme for agencies' destruction of telecommunications data. Agencies may destroy this information at their discretion and are not required to keep records of the process. In contrast, Chapters 2 and 3 of the TIA Act prescribe strict frameworks for the destruction of telecommunications interception and stored communications information, respectively.[20] However, these destruction frameworks place inconsistent obligations on agencies. During our inspections under the TIA Act, we routinely identify instances of non-compliance with destruction requirements, which arises largely as a result of these legislative inconsistencies.

Despite the use of telecommunications interception being a similarly intrusive covert power, the destruction of those records is subject to less stringent requirements than those required for stored communications. For telecommunications interception records, agencies are only required to destroy the original record of the telecommunications interception and not any copies subsequently made. Conversely, for stored communications records agencies must destroy the original record as well as all copies.

Under both frameworks, the chief officer must cause the destruction of the records 'forthwith' but this term is not defined in the TIA Act. There is also no provision allowing the chief officer to delegate this obligation.

Agencies have expressed frustration with these inconsistencies, the ambiguity surrounding the timeframe of 'forthwith' and the onus placed on chief officers to personally cause each destruction. We acknowledge it is often operationally problematic for agencies to meet these requirements. For example, some agencies have relied upon an implied authorisation for the chief officer to authorise other persons within the agency to approve the destruction of records. For these

[17] State and Territory agencies' use of the telecommunications interception powers under Chapter 2 of the TIA Act is overseen by a State or Territory inspecting body.
[18] Under Chapter 2, our Office provides an annual summary of our inspections of agencies' use of telecommunications interception powers. The Minister then uses that content to prepare his/her annual report regarding the TIA Act.
[19] See TIA Act, ss 84 and 85. A de-sensitised summary of our inspection findings are included in the Minister's annual report under s 99.
[20] See TIA Act, ss 79, 79A and 150.

reasons, when assessing destructions we rely on an agency's policy and procedural documents to determine compliance.

To ensure consistency, the Office would welcome the alignment of the destruction frameworks under the TIA Act, particularly the:

- **term 'forthwith' being defined to clarify what timeframe agencies are expected to destroy records within**
- **either destruction requirements for Chapter 2 being extended to copies of information or the destruction requirements for Chapter 3 records being limited to original records, and**
- **the destruction frameworks including a provision to allow the chief officer to delegate their obligation to cause each destruction.**

Retention of stored communications for the purposes of an Ombudsman inspection

Further to the above, currently under the TIA Act, agencies are not required to retain stored communications obtained under a warrant for the purpose of an Ombudsman inspection. In the majority of instances agencies have retained these records and we have been able to assess them. However, where agencies have destroyed stored communications prior to our inspection, we are unable to check whether that information complied with the relevant warrant.

The Committee may wish to consider whether there is a need for the record-keeping requirements under s 151 of the TIA Act to be expanded to require that agencies retain the stored communications they obtain under a warrant for the purposes of an Ombudsman inspection.