COMMONWEALTH OMBUDSMAN

A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the *Telecommunications (Interception and Access) Act 1979*

Compliance with Journalist Information Warrant provisions

Report by the Commonwealth Ombudsman
under the *Telecommunications (Interception and Access) Act 1979*

January 2019

COMMONWEALTH OMBUDSMAN

A report on the Commonwealth Ombudsman's inspection of the Australian Federal Police under the *Telecommunications (Interception and Access) Act 1979*

Compliance with Journalist Information Warrant provisions

Report by the Commonwealth Ombudsman
under the *Telecommunications (Interception and Access) Act 1979*

January 2019

ISBN: 978-0-9775288-5-1

Contact us
Inquiries regarding the licence and any use of this report are welcome at:

Commonwealth Ombudsman
Level 5, 14 Childers Street
Canberra ACT 2600
Tel: 1300 362 072
Email: ombudsman@ombudsman.gov.au

CONTENTS

EXECUTIVE SUMMARY

On 28 April 2017 the Australian Federal Police (AFP) Commissioner, Andrew Colvin, made a public statement to disclose the AFP had committed a breach of the *Telecommunications (Interception and Access) Act 1979* (the Act). The breach, which occurred within the Professional Standards Unit (PRS), involved access to the telecommunications data (broadly known as 'metadata') of a journalist for the purpose of identifying the journalist's source without a Journalist Information Warrant.

Telecommunications data is information about a communication which does not include its content. By way of an example, telecommunications data for a phone call may include the phone numbers of the two parties to the conversation and the duration, date and time of the phone call, but not what the parties said.

On 5 May 2017, in response to the AFP's disclosure, the Office of the Commonwealth Ombudsman conducted a non-routine inspection under Chapter 4A of the Act to examine the breach. The Ombudsman published a report in October 2017, which outlined the findings from the inspection and made suggestions and recommendations for improvement.

Between 5 and 7 September 2018 we conducted a second non-routine inspection at the AFP. This inspection was to examine the way the AFP had used the Journalist Information Warrants since the first inspection and assess its progress in implementing the recommendations and suggestions from our October 2017 report.

At the September 2018 inspection, we noted two exceptions to adherence with the conditions of a warrant but were otherwise satisfied the AFP had appropriately applied the Journalist Information Warrant provisions in the instances we inspected.

We identified that the AFP had made a number of procedural and process improvements since the October 2017 report. These included mandatory training, an increase in the level of seniority required to grant authorisations, improved operating procedures and improved visibility of information for staff about the Journalist Information Warrant provisions.

Although the AFP has made progress, one suggestion from our October 2017 report has not been implemented. Specifically, we had suggested that PRS staff undergo supplementary induction training relating to telecommunications data, shortly after commencing in the section.

We will continue to monitor the AFP's compliance with telecommunications data legislation through our routine inspections. We will also use those inspections to assess the AFP's progress in implementing our remaining suggestion.

PART 1: INTRODUCTION AND SCOPE

The legislation

1.1. Under s 180H of the Act, before an enforcement agency makes a telecommunications data authorisation for the purpose of identifying a journalist's source, it must first obtain a Journalist Information Warrant.

1.2. The requirement to obtain a Journalist Information Warrant was introduced as part of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act), which commenced on 13 October 2015. A summary of the legislation is provided at Appendix A.

1.3. The Journalist Information Warrant provisions were introduced into the Act in recognition of the public interest in protecting journalists' sources while ensuring agencies have the investigative tools necessary to protect the community. The provisions require an application to be made to an issuing authority such as an eligible Judge or Administrative Appeals Tribunal Member. Applications for a Journalist Information Warrant are also subject to scrutiny by a Public Interest Advocate, who is appointed by the Prime Minister under the Act. These oversight mechanisms aim to ensure that access to such data is only permitted in circumstances where the public interest in the issuing of the Journalist Information Warrant outweighs the public interest in maintaining the confidentiality of the source.

The disclosure

1.4. On 26 April 2017 the Australian Federal Police (AFP) advised the Office of the Commonwealth Ombudsman (the Office) it had breached the Act by accessing telecommunications data pertaining to a journalist without obtaining a Journalist Information Warrant.

1.5. On 28 April 2017 the AFP Commissioner, Andrew Colvin, made a public statement to disclose the breach.

First non-routine inspection

1.6. In response to the AFP's disclosure, on 27 April 2017 the acting Commonwealth Ombudsman wrote to the AFP to advise the Office would conduct an inspection on 5 May 2017 to examine the circumstances of the breach.

1.7. The May 2017 inspection was specific to the disclosed breach. It focused on understanding how the breach occurred and assisting the AFP to ensure the risk of future breaches was mitigated. Although the inspection commenced on 5 May 2017, activities associated with the inspection continued until early August 2017. For the

purposes of this report, the May 2017 inspection is referred to as the 'first non-routine inspection'.

1.8. During the first non-routine inspection, we interviewed staff who were directly and indirectly involved in the breach including reviewing, authorising and/or provisioning the request on the telecommunications carrier (the carrier). We also interviewed staff from another agency who had visibility of the investigation to which the breach related.

1.9. Both during, and subsequent to the first non-routine inspection, the AFP provided our Office with supporting records and documentation, including policies and procedures which had been reviewed and/or updated in light of the breach.

1.10. We also reviewed supporting documentation relating to the events leading up to, and subsequent to the breach being identified. At the first non-routine inspection, we inspected records relating to four telecommunications data authorisations associated with the breach.

October 2017 report

1.11. In October 2017 our Office released a public report, detailing the findings of the first non-routine inspection.

1.12. In that report, our Office concluded there were four main factors which had contributed to the breach:

- at the time of the breach, there was insufficient awareness surrounding Journalist Information Warrant requirements within the AFP's Professional Standards Unit (PRS)
- within PRS, a number of officers did not appear to fully understand their responsibilities when exercising telecommunications data powers
- the AFP relied heavily on manual checks and corporate knowledge because it did not have strong system controls in place to prevent applications that did not meet relevant thresholds from progressing
- although guidance documents were updated prior to the commencement of the Journalist Information Warrant provisions in 2015, they were not effective as a control to prevent the breach.

1.13. Our report noted the AFP's transparency in making the disclosure to our Office and concluded the AFP had adequately managed the telecommunications data that had been unlawfully accessed. In our view the remedial measures taken by the AFP by the

time of the first non-routine inspection went some way to ensuring a similar breach would not occur again.

1.14. As a lack of awareness amongst AFP staff had played a significant role in the breach, we made a formal recommendation:

"That the Australian Federal Police immediately review its approach to metadata awareness raising and training to ensure that all staff involved in exercising metadata powers have a thorough understanding of the legislative framework and their responsibilities under Chapter 4 of the Telecommunications (Interception and Access) Act 1979."

1.15. Our Office also made a number of suggestions to the AFP regarding how it could strengthen its existing controls. In response, the AFP advised it had already implemented some of these suggestions and would turn its attention to implementing the rest.

Inspection conducted during 2017–18

1.16. During the 2017–18 financial year our Office conducted one routine inspection of the AFP's access to telecommunications data. During this inspection we also monitored the AFP's progress in relation to the findings in the October 2017 report.

1.17. Our assessment of the AFP's progress in response to the report is included in this report, however our broader assessment of the AFP's compliance with the Act will be incorporated into our 2017–18 Annual Report. The Annual Report is to be provided to the Minister 'as soon as practicable' after 30 June 2018.

PART 2: SEPTEMBER 2018 NON-ROUTINE INSPECTION

Inspection objectives

2.1. Between 5 and 7 September 2018, our Office conducted a second non-routine inspection at the AFP. This inspection focused on assessing the AFP's compliance with the telecommunications data access provisions under Chapter 4 of the Act, specifically its application of the Journalist Information Warrant provisions.

Inspection scope

2.2. During the inspection our Office considered and assessed:

- all applications for Journalist Information Warrants since the first non-routine inspection
- all Journalist Information Warrants issued to the AFP since the first non-routine inspection
- each authorisation made under an expired or revoked Journalist Information Warrant since the first non-routine inspection.

2.3. Our Office also assessed the AFP's actions in response to the October 2017 findings, which are discussed in Part 3 of this report.

Inspection findings

2.4. Overall, we were satisfied the AFP had appropriately applied the Journalist Information Warrant provisions in the instances we inspected. We noted two exceptions to adherence with the conditions of the warrant which are discussed below.

2.5. We noted the AFP had drafted warrant conditions with the intent of setting clear limitations on authorisations that could be made, both to ensure the investigatory value of authorisations and to minimise any unnecessary privacy intrusion.

<u>Exception 1: Use of the Integrated Public Number Database</u>

2.6. The Integrated Public Number Database (IPND) is a telecommunications industry database containing all listed and unlisted public telephone numbers and can be searched after making an authorisation to access telecommunications data.

2.7. During our inspection, we identified instances where IPND searches provided data results beyond the date range specified in the warrant conditions.

2.8. While the data returned in response to some IPND searches did not explicitly comply with the warrant conditions, we noted this was the result of limitations of the IPND interface, which does not allow users to limit searches to a specified date range.

2.9. Given these limitations, we acknowledged that compliance with the warrant conditions for IPND was impractical.

2.10. We note the AFP's proactive approach to mitigating privacy intrusion by drafting warrant conditions. In future we suggest the AFP also ensures any warrant conditions can be given practical effect before they are finalised.

2.11. Following the inspection, the AFP advised that its guidance on obtaining Journalist Information Warrants will be updated to require officers to consider the impact of warrant conditions prior to issue. AFP also advised that it has begun using this issue as an example in training; highlighting the need to ensure restrictions placed on warrants or authorisations are compatible with telecommunication request systems.

Exception 2: Access to subscriber information

2.12. Under an authorisation for telecommunications data, an agency can access various types of information from carriers, including subscriber information. Subscriber information is information held by a carrier relating to those who are subscribed to its services including details such as the subscriber's name and address.

2.13. During our inspection, we identified three authorisations for access to subscriber information where the requests did not limit the date range for results as per the warrant conditions.

2.14. As with the IPND, it is carriers' usual practice to provide current information about the status of a service when responding to a request for subscriber information. While the requests above did not specify a date range, we note the information returned as a result of these requests was still compliant with the conditions of the warrant in these instances.

2.15. We note that subsequent authorisations made were specific to warrant conditions and, in some cases, contained additional text to appropriately narrow the scope of the request.

2.16. With the exception of the three instances above, where a date range was not specified, we concluded the AFP had demonstrated a strong awareness of the warrant conditions in making authorisations to access subscriber information.

PART 3: ASSESSMENT OF THE AFP'S RESPONSE TO THE BREACH

3.1. In our October 2017 report we identified four main factors which led to the AFP's breach of the Journalist Information Warrant provisions of the Act:

- at the time of the breach, there was insufficient awareness surrounding Journalist Information Warrant requirements within the AFP's PRS
- within PRS, a number of officers did not appear to fully understand their responsibilities when exercising telecommunications data powers
- the AFP relied heavily on manual checks and corporate knowledge because it did not have strong system controls in place to prevent applications that did not meet relevant thresholds from being progressed
- although guidance documents were updated prior to the commencement of the Journalist Information Warrant provisions in 2015, they were not an effective control to prevent this breach.

3.2. During the routine inspection conducted in 2017–18 and the second non-routine inspection conducted in September 2018, our Office assessed the AFP's actions to address these factors.

Awareness of Journalist Information Warrant provisions

3.3. Despite the AFP's efforts to raise awareness, it was evident during the first non-routine inspection that, prior to the breach being identified, a number of staff within PRS were not aware of the Journalist Information Warrant provisions. In our view, the likely reasons for this were:

- raising awareness through email and intranet announcements was not sufficiently direct to be effective
- PRS infrequently exercised telecommunications data powers
- the rotational nature of PRS staffing, which has an impact on retaining corporate knowledge and increases the need for contemporaneous and comprehensive training
- PRS operates separately from the rest of the AFP and has its own processes for provisioning telecommunications data requests
- AFP training and awareness raising activities were aligned to the commencement of the Data Retention Act in October 2015. This means that staff commencing with the AFP, and staff changing roles within the AFP since 2015 would not have had the same exposure to information about the

legislative amendments. This places greater emphasis on the need for stronger embedded process controls, as outlined below

- PRS has an ad-hoc induction training schedule.

3.4. During the first non-routine inspection, PRS advised it conducted induction training for new staff within PRS, but only once there were enough inductees to warrant running a session. This means a newcomer may not receive formal induction training until several months after they commence with PRS. At the time of our first non-routine inspection, PRS induction did not specifically address telecommunications data powers.

3.5. In our October 2017 report, we suggested the AFP implement a supplementary induction training package that PRS new-starters must complete prior to commencing with PRS if the formal induction is likely to be delayed. We suggested this supplementary training package cover roles and responsibilities for telecommunications data, and specifically highlight the higher thresholds for applications relating to journalists.

3.6. At our second non-routine inspection, this suggestion had not been implemented by the AFP. PRS staff still do not complete formal telecommunications data training until they are formally inducted into PRS, which may occur many months after they commence. Given that we identified training for PRS staff as a particular risk in our October 2017 report, we are concerned this suggestion has not yet been acted on.

3.7. Following the inspection, the AFP proposed to introduce a mandatory online training program for requesting officers in 2019. The aim of this training will be to foster a heightened awareness of the Journalist Information Warrant provisions under the Act for all requesting officers, including those in PRS. In December 2018 the AFP also updated PRS's New Starter Induction Checklist. This new checklist is to be completed when staff commence in PRS and records their acknowledgement of general guidance material related to telecommunications data as well as specific information about the Journalist Information Warrant provisions.

3.8. In our October 2017 report, we also made the following formal recommendation in relation to awareness of Journalist Information Warrant provisions:

"That the Australian Federal Police immediately review its approach to metadata awareness raising and training to ensure that all staff involved in exercising metadata powers have a thorough understanding of the legislative framework and their responsibilities under Chapter 4 of the Telecommunications (Interception and Access) Act 1979."

3.9. In response to this recommendation, the AFP advised it was finalising an online mandatory training package that all AFP authorised officers will need to complete annually to maintain their status as an authorised officer.

3.10. The AFP has since implemented mandatory training for AFP authorised officers regarding access to telecommunications data. At the second non-routine inspection our Office confirmed that all authorised officers had attended this course, and was satisfied the AFP had appropriate measures in place to assure itself all authorised officers had completed the training.

3.11. To gauge the level of awareness of Journalist Information Warrant provisions, during the second non-routine inspection, we spoke with officers involved in all stages of applying for, reviewing, authorising and provisioning the requests for telecommunications data on the carrier. As a result of those discussions, as well as the processes we observed, we were satisfied that, in the instances we inspected, officers demonstrated a good understanding of the requirements of the Act.

3.12. Our Office will continue to monitor the AFP's implementation of this recommendation at future inspections with the aim of assessing the effectiveness of the AFP's remedial actions across the agency.

Personal accountability when exercising telecommunications data powers

3.13. The AFP's process for exercising telecommunications data powers, like many other enforcement agencies, is spread across different staff. Generally, the process involves an applicant, an authorised officer, a person or team to liaise with the carrier regarding the access and any quality assurance roles.

3.14. During inspections, it is our practice to examine the level of personal accountability each officer of the agency demonstrates when exercising telecommunications data powers. Agencies that demonstrate high levels of personal accountability in the exercise of powers across all roles and levels are generally considered to have a strong compliance culture.

3.15. In our October 2017 report we noted that not all PRS officers fully understood the legislative framework in which they were operating when exercising telecommunications data powers. In many instances this function was not a frequent or substantial part of their duties which, in turn, meant their approach tended to be process based and lacked an understanding of the broader legislative requirements.

3.16. We have identified that, where all staff involved in the exercise of telecommunications data powers at an agency have a sound understanding of the associated legislative framework, it acts not only to minimise the likelihood of errors but also to increase the likelihood of any errors or omissions that do occur being identified and addressed.

3.17. Whilst the second non-routine inspection did not cover any authorisations made, or Journalist Information Warrants issued to PRS, the officers involved in the instances we inspected demonstrated an appropriate level of personal accountability when exercising telecommunications data powers.

3.18. Our Office will continue to monitor the level of personal accountability demonstrated by officers of the AFP at future inspections.

Process controls

3.19. During the first non-routine inspection, AFP staff were receptive to stronger controls being embedded into template documents, to ensure compliance with s 180H of the Act. As part of the AFP's response to the breach, it updated its templates so that, where an officer seeks to identify a journalist's information source, they are alerted to the process for making Journalist Information Warrant applications. This prompt acts as a control on all authorisation applications submitted using the updated template.

3.20. After reviewing the new templates, and based on insights gained from oversight of other enforcement agencies, in our October 2017 report we suggested the prompt be strengthened. As it currently stands, the prompt is specific to applications seeking to identify a journalist's source. We suggested the prompt capture a broader range of scenarios and be expanded to include any instance where it is reasonably believed that an application relates to a journalist. This would prompt the AFP's governance and legal areas to consider a wider range of scenarios when assessing the need to obtain a Journalist Information Warrant.

3.21. Since our first non-routine inspection, the AFP has implemented a number of measures to ensure that, where an application relates to a journalist, appropriate considerations are made. Specifically, it has implemented mandatory training for authorised officers on access to telecommunications data and prominent display of Journalist Information Warrant guidance. Our Office will continue to monitor the effectiveness of these measures at future inspections.

3.22. As discussed in our October 2017 report, the AFP also relies on a number of other controls to achieve legislative compliance, including a review mechanism to identify deficiencies in telecommunications data authorisations before they are provisioned on the carrier. In our view, this mechanism acts as a sound control to prevent deficient authorisations from progressing, by ensuring that, for example, the correct forms are used, relevant offence thresholds are met and the authorised officer is not the same person as the requesting officer. The information collated through this mechanism may also inform future training activities.

3.23. In our October 2017 report we suggested this mechanism be expanded to incorporate a check to ensure that any telecommunications data authorisations relating to journalists have a corresponding Journalist Information Warrant.

3.24. The AFP has since expanded this quality assurance mechanism by incorporating a check to ensure that any telecommunications data authorisations relating to journalists are accompanied by a Journalist Information Warrant. We note this additional check still relies upon the requesting officer and the authorised officer to identify and disclose that the authorisation is sought in relation to a journalist for the purpose of identifying that journalist's source.

Guidance documents

3.25. In our October 2017 report, we also suggested the AFP review its guidance and template documents to incorporate links to relevant guidance and instructional materials.

3.26. The AFP has developed new standard operating procedures and authorisation prompts that alert officers to the relevant requirements of the Act, including the Journalist Information Warrant provisions. The AFP also increased the level of seniority required for officers to make authorisations under a Journalist Information Warrant.

3.27. The AFP can also make authorisations for foreign law enforcement. It provides guidance materials for issuing such authorisations, however, the only reference to the Journalist Information Warrant provisions appears to be in the authorised officer checklist. That checklist notes that s 180H(2) of the Act precludes the issuing of a foreign law enforcement authorisation in relation to a journalist or their employer, to identify the source of a journalist.

3.28. In our October 2017 report we suggested the AFP strengthen its controls to include the s 180H(2) prohibition throughout the foreign law enforcement guidance document and associated templates.

3.29. At our second non-routine inspection we noted the foreign law enforcement guidance document now advises there is no provision for disclosing telecommunications data access under a Journalist Information Warrant through a foreign law enforcement authorisation. There are also prompts on the authorisation document to remind officers of this prohibition.

PART 4: CONCLUSIONS

4.1. The Journalist Information Warrant provisions were introduced into the Act to ensure that access to telecommunications data to identify a journalist's source is only permitted if the public interest in doing so outweighs the public interest in maintaining the confidentiality of a journalist's source.

4.2. In our view, the AFP respects this higher threshold for journalists and takes its legislative obligations seriously, particularly in relation to its use of covert and intrusive powers.

4.3. In the instances we inspected at the second non-routine inspection, the AFP had appropriately applied the Journalist Information Warrant provisions and, with the exception of one issue discussed in the body of this report, was compliant with the requirements of the Act.

4.4. Our Office notes the AFP's progress in addressing the issues raised in our October 2017 report. We will continue to monitor the AFP's implementation of the outstanding suggestion through our routine inspections, the results of which will be included in our Annual Report to the Minister.

APPENDIX A: LEGISLATIVE BACKGROUND

The *Telecommunications (Interception and Access) Act 1979* (the Act) provides a legislative framework for agencies to lawfully receive information from carriers, including through telephone interception, access to stored communications such as Short Messaging Service (SMS) and through the disclosure of telecommunications data.

Telecommunications data, or metadata, is information about a communication which does not include the contents of a communication. In the example of a phone call, telecommunications data may include the phone numbers of the two parties to the conversation, the duration, date and time of that phone call but not what was said.

Enforcement agencies may internally authorise the disclosure of telecommunications data if it is reasonably necessary for the enforcement of the criminal law, to locate a missing person or to enforce a law imposing a pecuniary penalty or for the protection of public revenue.

On 13 October 2015, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act) commenced, introducing a requirement for carriers to retain telecommunications data for a minimum period of two years.

For agencies seeking to access telecommunications data, new requirements were imposed on agencies to increase the privacy threshold for which an authorised officer must be satisfied prior to internally issuing an authorisation.

The Data Retention Act also established an independent oversight function for the Commonwealth Ombudsman in relation to the exercise of powers under Chapter 4 of the Act by enforcement agencies.

Of particular note are the new requirements regarding Journalist Information Warrants under Division 4C, Chapter 4 of the Act, which apply when an enforcement agency seeks to access the telecommunications data of a journalist for the purpose of identifying another person whom is reasonably believed to be a source of that journalist. In such instances, an enforcement agency must obtain a Journalist Information Warrant prior to making an authorisation to access that information.

To obtain a Journalist Information Warrant, an enforcement agency must apply externally to an eligible Judge, Magistrate or Administrative Appeals Tribunal member, who has been appointed by the Minister.[1]

The issuing authority must not issue a Journalist Information Warrant unless they are satisfied, for example, that the warrant is reasonably necessary for the enforcement of the

[1] A full list of Part 4-1 issuing authorities is at section 6DC of the Act.

criminal law and that the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source in connection with whom authorisations would be made under the authority of the warrant.[2]

Journalist Information Warrants are also subject to scrutiny from a Public Interest Advocate, who is appointed by the Prime Minister. Under the Act, the Public Interest Advocate may make submissions to an eligible issuing authority about matters relevant to the decision to issue, or refuse to issue, a Journalist Information Warrant.

Once a Journalist Information Warrant is issued, the enforcement agency must, as soon as practicable, provide a copy of the warrant to the Commonwealth Ombudsman. If the agency is the AFP, it must also provide a copy of the warrant to the Minister, who must then cause the Parliamentary Joint Committee on Intelligence and Security (the Committee) to be notified of the issuing of the warrant.[3]

Journalist Information Warrant provisions were the subject of consideration in the Committee's advisory report on the Telecommunications (Interception and Access) Bill 2014, released in February 2015, and the Committee's Inquiry into the authorisation of access to telecommunications data to identify a journalist's source.[4]

[2] Section 180T of the Act stipulates the considerations that an issuing authority must be satisfied of when issuing a Journalist Information Warrant.
[3] Section 185D(5) details an agency's notification obligations in relation to Journalist Information Warrants.
[4] The Parliamentary Joint Committee on Intelligence and Security reports can be accessed at: http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report; and http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/access_to_journalists_dat