COMMONWEALTH OMBUDSMAN

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

Report by the Commonwealth Ombudsman,
Michael Manthorpe PSM
under the *Telecommunications (Interception and Access) Act 1979*

October 2017

COMMONWEALTH OMBUDSMAN

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

Report by the Commonwealth Ombudsman,
Michael Manthorpe PSM
under the *Telecommunications (Interception and Access) Act 1979*

October 2017

ISBN 978-0-9875235-6-3

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 APM OAM, held a press conference to disclose that a breach of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) had occurred within the AFP. The breach occurred within the Professional Standards Unit (PRS) and involved access to the telecommunications data (metadata) of a journalist for the purpose of identifying the journalist's source without a warrant.

Metadata is information about a communication which does not include its content. In the example of a phone call, metadata 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.

On 13 October 2015, a higher threshold was introduced for instances where metadata was being sought in relation to a journalist for the purpose of identifying that journalist's source. The Journalist Information Warrant provisions were introduced into the TIA Act in recognition of the public interest in protecting journalists' sources while ensuring agencies have the investigative tools necessary to protect the community. These provisions require an application to be made to an issuing authority such as an eligible Judge or Administrative Appeals Tribunal Member. Applications for a warrant are also subject to scrutiny by a Public Interest Advocate, who is appointed by the Prime Minister under the TIA 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 warrant outweighs the public interest in maintaining the confidentiality of the source.

Prior to the Commissioner's press conference, on 25 April 2017 the AFP voluntarily disclosed this matter to the Commonwealth Ombudsman's Office, outside of our formal inspections program. This was followed by a formal letter to our Office on 26 April 2017. Our Office notified the AFP of our intent to conduct an inspection under the TIA Act regarding the breach, which was conducted on 5 May 2017.

As a result of our inspection, we confirmed that the AFP had breached the TIA Act in that it did not obtain a Journalist Information Warrant prior to accessing metadata of a journalist for the purpose of identifying the journalist's source.

Overall, there appeared to be four main factors which contributed to this breach:

- at the time of the breach, there was insufficient awareness surrounding Journalist Information Warrant requirements within PRS
- within PRS, a number of officers did not appear to fully appreciate their responsibilities when exercising metadata powers

- the AFP relied heavily on manual checks and corporate knowledge as it did not have in place strong system controls for preventing 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, they were not effective as a control to prevent this breach.

In response to the notified breach, the AFP has responded appropriately and effected suitable remedial action, notably:

- immediately quarantining the unlawfully accessed data and seeking legal advice

- taking action to limit any direct and indirect use of the unlawfully accessed data, including destroying that data

- reviewing investigations conducted within PRS to confirm that there have been no other breaches of this nature within that unit

- implementing AFP-wide changes to prevent a future recurrence, including: requiring mandatory training for authorised officers; raising the level of seniority for authorised officers who may issue authorisations under Journalist Information Warrants and thereby limiting the number of people who may issue an authorisation in those circumstances; amending its templates; reviewing its standard operating procedures and guidance documents and reminding all staff about the requirement to obtain a Journalist Information Warrant in the relevant circumstances.

As a result of our inspection we make the following key recommendation:

Recommendation 1
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*.

In response to this recommendation, the AFP advised that it is now finalising an online mandatory training package that all AFP authorised officers will need to undertake annually to maintain their authorised officer status. We will monitor the AFP's implementation of this recommendation, particularly in relation to how it assures itself that all authorised officers have completed the training. We will also monitor how the recommendation is applied to all staff involved in the exercise of metadata powers, not just authorised officers.

We have also made a number of suggestions to the AFP regarding how it can strengthen its existing controls to prevent another breach of a similar nature. In response to this, the AFP advised that it has already implemented some of these suggestions and will turn its attention to implementing all of them. We will monitor the implementation of the suggestions in this report at our 2017-18 metadata inspection of the AFP.

During the course of our inspection, we also identified that there is ambiguity surrounding the circumstances of when a Journalist Information Warrant is required. It appears that the intention of the Journalist Information Warrant provisions is to require a warrant prior to authorising the disclosure of metadata to identify a journalist's source. It is arguable, however, that those provisions only apply in the more limited circumstance where the authorisation is seeking to access the metadata of a journalist or their employer. That is, if an authorisation was issued for the purpose of identifying a journalist's source but is not made directly in relation to that journalist or their employer, a warrant is not required.

There were four authorisations associated with this breach: one was a clear breach and it is arguable whether the other three breached the relevant provisions of the TIA Act. By the time of our inspection, the AFP had taken remedial action in relation to all four authorisations to limit any direct or indirect use of the obtained metadata.

During the inspection, we also identified the role that an external agency played in identifying this breach at the AFP. Although the possibility of a breach was considered during an internal AFP review of the relevant investigation, as publicly advised by the Commissioner on 28 April 2017, based on the information provided to us, it appears that it was due to a prompt by that external agency that the relevant officer in the AFP reviewed the relevant investigation.

The AFP provided our Office with full and free access to relevant staff and information during the course of our inspection. We acknowledge the AFP's cooperation, openness and transparency with our Office in both the way it has voluntarily disclosed the breach and throughout our inspection. We particularly acknowledge the high level of personal accountability demonstrated by the authorised officer directly involved once the breach was identified.

PART 1: INTRODUCTION AND SCOPE

Introduction

1.1. On 26 April 2017, the AFP advised the Commonwealth Ombudsman's office that it had breached the TIA Act, as it had accessed metadata pertaining to a journalist without obtaining a Journalist Information Warrant.

1.2. Under s 180H of the TIA Act, prior to an enforcement agency issuing a metadata authorisation for the purpose of identifying a journalist's source, it must first obtain a Journalist Information Warrant. An application for such a warrant must be made to an issuing authority such as an eligible Judge or Administrative Appeals Tribunal Member. The application is also subject to scrutiny by a Public Interest Advocate, who is appointed by the Prime Minister under the TIA Act.

1.3. 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.

1.4. In response to the AFP's voluntary disclosure, on 27 April 2017 the acting Commonwealth Ombudsman wrote to the AFP advising that our Office would conduct an inspection regarding the breach on 5 May 2017.

Scope of inspection and methodology

1.5. This report does not comment on the policy rationale behind the Data Retention Act or the provisions regarding Journalist Information Warrants.

1.6. Although we acknowledge the seriousness and gravity of the investigation being conducted by the AFP, we cannot comment on whether the AFP would have been granted a Journalist Information Warrant if it had applied for one, as this would have been at the discretion of the eligible issuing authority.

1.7. The Commonwealth Ombudsman's role is to assess agencies' compliance with the legislative framework for the use of certain covert and intrusive powers, including when they may be compliant yet out-of-step with the intention of Parliament.

5 May Inspection

1.8. This inspection was specific to the voluntarily disclosed breach, focusing on understanding how the breach occurred and assisting the AFP to ensure that future breaches are mitigated. Although the inspection commenced on 5 May 2017, inspection activities continued until early August 2017. For the

purpose of this report, this inspection will be referred to as the "5 May Inspection".

1.9. During the 5 May Inspection, the AFP provided our Office with full access to relevant staff. We interviewed staff who were directly and indirectly involved in the breach. This included staff who were involved in the stages of applying for, reviewing, authorising and provisioning the request on the carrier. We also interviewed staff from another agency who had visibility over the investigation which the breach affected.

1.10. Both during and subsequent to the 5 May 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. We also reviewed supporting documentation relating to the events leading up to, and subsequent to, the breach being identified. At the 5 May Inspection, we inspected relevant records relating to all four metadata authorisations associated with the breach.

Health check inspection

1.11. This report does not examine the AFP's broader compliance framework for the exercise of its metadata powers. This broader assessment of the AFP was conducted in November 2015, during our 'health check' inspection. The report on our findings from that inspection was tabled by the Commonwealth Attorney-General in Parliament on 22 May 2017 and can be accessed on our Office's website.[1]

1.12. During our 2015-16 health check inspections of all 20 enforcement agencies, we focused on understanding the policies and procedures in place at each agency in relation to exercising metadata powers. We used this understanding to subsequently assess individual records at each agency for compliance.

1.13. As a result of the AFP's health check inspection, we were satisfied that the AFP had a sufficient framework in place to ensure appropriate access to metadata. However, we identified a number of risks for the AFP, which we discuss in the body of this report.

1.14. It is our usual practice to monitor progress on remedying issues and identified risks at each subsequent inspection. At the time of receiving the AFP's self-

[1] The report can be accessed at: http://www.ombudsman.gov.au/__data/assets/pdf_file/0018/45423/TIA-Act-Annual-Report-2015-16.pdf

disclosure, we had not yet conducted our scheduled metadata inspection at the AFP for 2016-17.

1.15. By the time of our 5 May Inspection, the metadata processes within PRS had changed since our November 2015 health check inspection. During the health check, PRS had not yet transitioned to the new database implemented by the wider AFP. Therefore, during and subsequent to the 5 May Inspection, we updated our understanding of the internal processes used by PRS for accessing metadata.

Routine inspection

1.16. Under the TIA Act, the Ombudsman must inspect records of each enforcement agency to determine the extent of legislative compliance with the metadata provisions by the agency and its officers. In relation to metadata, the Commonwealth Ombudsman conducts annual inspections to assess enforcement agencies' compliance with Chapter 4 of the TIA Act.

1.17. For the AFP, this routine inspection of individual records was scheduled to occur after 5 May 2017. For the purpose of this report, this subsequent inspection will be referred to as the "Routine Inspection".

1.18. The results of the 5 May Inspection will be presented in this report and the results of the Routine Inspection will be reported on in the Commonwealth Ombudsman's 2016-17 annual report to the Minister, which the Minister must then present to Parliament.

1.19. Although the 5 May Inspection and the Routine Inspection were conducted separately, information from both inspections informed this report. Both inspections were conducted using the same methodology, involving an inspection of relevant records as well as interviews with staff and an observation of processes as they are being applied by staff.

1.20. This report is also informed by our experience in inspecting 20 law enforcement agencies' compliance with a range of covert and intrusive powers. As a result, we have gained a detailed understanding of how different agencies apply such powers and the common areas of legislative compliance risk. Specific to this report, we draw on our experience in regularly inspecting the AFP against legislation pertaining to a range of different powers and functions.

PART 2: INSPECTION RESULTS

Inspection objectives

2.1. On 5 May 2017, we conducted an inspection regarding the AFP's voluntarily disclosed breach of the TIA Act. The objectives of the 5 May Inspection were to:

- identify the circumstances surrounding the breach
- assess the AFP's compliance with Chapter 4 of the TIA Act
- capture the AFP's remedial actions
- assess the likelihood of another breach of a similar nature occurring again at the AFP
- identify any areas for improvement.

Inspection findings

2.2. Section 180H of the TIA Act states that 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.

Compliance assessment

2.3. The 5 May Inspection confirmed that the AFP had breached s 180H of the TIA Act.

2.4. As a part of our inspection, we usually check to ensure that the metadata received by the agency was within the scope of the request and that there was no content received as a result of that authorisation. However, as the relevant

data had already been destroyed by the AFP prior to the 5 May Inspection, we did not conduct this check.

2.5. As a result of our inspection, we also identified that not all copies of records containing the unlawfully accessed data had been destroyed by the AFP.

2.6. In relation to the destruction of all copies of records containing the unlawfully accessed data, the AFP advised our Office that it had destroyed all of the material that was provided to it as a result of the breach. However, to confirm that this had been done, we arranged to revisit the AFP with technical assistance, appreciating the complexities of the AFP's systems. This visit prompted PRS to conduct further checks of its systems with technical assistance, which identified additional records. We confirmed that these records were subsequently destroyed.

2.7. As a result of the above activities, we are satisfied that the AFP has destroyed and appropriately managed all material obtained under the relevant authorisations. We note that the AFP has kept the relevant authorisation instrument, as it is required to be kept for record-keeping purposes under s 186A of the TIA Act.

2.8. Nevertheless, we suggest that AFP, when destroying information, seek assistance from its technical officers to ensure that the information is destroyed from all locations on its systems.

Number of breach instances

2.9. During the course of our inspection, we identified that there is ambiguity surrounding the circumstances of when a Journalist Information Warrant is required. It appears that the intention of the Journalist Information Warrant provisions is to require a warrant prior to authorising the disclosure of metadata to identify a journalist's source. It is arguable, however, that those provisions only apply in the more limited circumstance where the authorisation is seeking to access the metadata of a journalist or their employer. That is, if an authorisation was issued for the purpose of identifying a journalist's source but is not made directly in relation to that journalist or their employer, a warrant is not required.

2.10. The Commonwealth Attorney-General's Department (AGD) has issued guidance to agencies in relation to Journalist Information Warrants. The guidance does not expressly address the application of Journalist Information Warrant provisions in these circumstances, however, does lend itself to a broader interpretation of the provisions; that is, that a warrant is required prior to authorising the disclosure of metadata for the purpose of identifying a journalist's source.

2.11. There were four authorisations associated with this breach:

- one authorisation that was in clear breach of s 180H of the TIA Act, in that it was in relation to the journalist for the purpose of identifying that journalist's source
- one authorisation that preceded the above authorisation and was in relation to the journalist, but did not directly identify that journalist's source
- two authorisations that were issued subsequent to the authorisation in breach that were not directly made in relation to the journalist (or their employer) but were for the purpose of identifying that journalist's source.

2.12. It is arguable whether three of the above four authorisations (the one preceding and the two subsequent) breached the relevant provisions of the TIA Act. In any event, by the time of our inspection, the AFP had taken remedial action in relation to all four authorisations to limit any direct or indirect use of the obtained metadata.

The AFP's response to the breach

2.13. In our opinion, the AFP has responded appropriately to the breach of s 180H of the TIA Act.

2.14. We found no evidence to counter the AFP's assessment that the breach was a mistake with no ill will, malice or bad intent involved.

2.15. With regards to how the breach was identified, based on our understanding of the events leading up to the voluntary disclosure to our Office, it appears that an external agency initially prompted the AFP to review the relevant investigation, resulting in consideration of the relevant legislative requirements.

2.16. In responding to this breach, the AFP undertook the below activities.

- The AFP reviewed its PRS investigations into unauthorised release of information since the commencement of the Data Retention Act to confirm that no other breaches of this nature had occurred within that unit.
- The AFP immediately quarantined the unlawfully accessed data and sought internal legal advice.
- Upon receiving legal advice, the AFP took immediate action to address the breach and implement changes to increase awareness, strengthen guidance documents and review metadata templates.

- The AFP took appropriate action to manage the risk of direct and indirect use of the metadata associated with the breach and took steps to cause the destruction of it (noting our comments under paragraph 2.5).
- On 28 April 2017, the AFP amended its policy in order to reduce the number of authorised officers who may issue metadata authorisations under Journalist Information Warrants. Delegation instruments were updated on 1 August 2017 to reflect this policy change.
- We note that this policy only relates to authorisations issued under Journalist Information Warrants, rather than all types of metadata authorisations.
- At the time of drafting this report, 190 authorised officers were delegated to issue metadata authorisations. Fifty-four of them could issue metadata authorisations under a Journalist Information Warrant.
- The AFP should consider the relevant training and experience of officers who may temporarily act in higher positions which have been delegated to issue metadata authorisations. These officers are not subject to mandatory metadata training and would have infrequently, if at all, issued metadata authorisations.
- As a result of our AFP metadata health check report, prior to this breach being identified, the AFP initiated a new requirement that all authorised officers must complete mandatory training and annual recertification prior to issuing metadata authorisations.
- The AFP advised that the training will serve to increase general knowledge and raise awareness as to best practice when authorising powers, including data authorisations. We understand that completion of this training will be monitored.
- At the time of drafting this report, this training package was under development. We offer to assist the AFP in reviewing this package before it is finalised.
- The AFP reviewed its standard operating procedures and guidance documents to include enhanced Journalist Information Warrant guidance.
- At the time of drafting this report, some of these documents were still under review.
- The AFP updated its smart form templates to include prompts for Journalist Information Warrants, which will prevent the progression of an application for authorisations in the relevant circumstances.

- The AFP distributed an all staff email reminder about metadata and the requirements when seeking to access metadata to identify a journalist source.

2.17. The AFP has been cooperative, open and transparent with our Office in the way it proactively and voluntarily disclosed the breach and throughout our subsequent inspection dealings.

PART 3: CONTRIBUTING FACTORS LEADING TO THE BREACH

3.1. As a result of the 5 May Inspection, our Office identified four main contributing factors which led to the AFP's breach of the Journalist Information Warrant provisions of the TIA Act:

- at the time of the breach, there was insufficient awareness surrounding Journalist Information Warrant requirements within PRS
- within PRS, a number of officers did not appear to fully appreciate their responsibilities when exercising metadata powers
- the AFP relied heavily on manual checks and corporate knowledge as it did not have in place strong system controls for preventing 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, they were not effective as a control to prevent this breach.

Awareness of Journalist Information Warrant provisions

3.2. As a result of our metadata health check inspections conducted across 20 enforcement agencies, we identified some common areas of risk for non-compliance with the TIA Act as amended by the Data Retention Act, which introduced the Journalist Information Warrant provisions. These risks include the timeliness and comprehensiveness of training given to those exercising metadata powers, and the effectiveness of internal communications within an agency to raise awareness of relevant changes and share best practices.

3.3. During the 5 May Inspection, it was noted by various officers throughout PRS that they were not aware of the new Journalist Information Warrant provisions.

3.4. During the health check inspection, it was noted that the AFP had prepared for the commencement of the Data Retention Act by preparing and making comprehensive training materials available to staff. In addition to awareness raising on the intranet, the AFP distributed an all staff email and utilised email

groups separately dedicated to applicants and authorised officers to distribute awareness raising materials.

3.5. At the time of the health check inspection, we noted that the AFP had no record of which officers had reviewed the awareness raising and training material sent via email. This posed a risk to ensuring that all relevant staff were aware of their new obligations when exercising metadata powers post 13 October 2015, being the commencement of the Data Retention Act.

3.6. We also noted that one staff member took a major lead in preparing the agency for the significant changes resulting from the Data Retention Act. Although the AFP did not establish a 'metadata working group' comprising representatives from all relevant areas within the agency, we acknowledged the experience of the officer taking the lead.

3.7. At other inspected enforcement agencies, metadata working groups were generally formed early on during the planning stage and comprised staff from the areas provisioning the different types of metadata requests (historic and prospective), legal, information technology and governance. These working groups proved effective in planning for the amendments and raising awareness throughout the agency of the new requirements.

3.8. Noting the challenges of reaching out to an organisation as large and dispersed as the AFP, the AFP adopted a mixed approach of raising awareness by: updating its intranet banner to draw attention to the new amendments during the month leading up to the amendments; amending its standard operating procedures and aid memoirs to reflect the new requirements; sending emails to the entire agency, as well as targeted emails to all applicants and all authorised officers, notifying them of the new amendments; and updating template documents. The AFP also adopted a new database to streamline its processes for metadata applications, authorisations, record keeping and reporting purposes.

3.9. We acknowledge the range of awareness raising activities adopted by the AFP during the preparation and implementation stages of the Data Retention Act. However, during the 5 May Inspection, the applicant for the relevant metadata authorisations advised that they had not received any formal training on metadata and instead, relied on the AFP intranet to understand the process in order to make the application.

3.10. Despite the AFP's awareness raising efforts, it was evident to us during the 5 May 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 are outlined below.

- The form of awareness raising through email and intranet announcements was not sufficiently direct to ensure its effectiveness.
- PRS infrequently exercised metadata 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 as a silo within the AFP and has its own processes for provisioning metadata 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 entering new roles within the AFP, since 2015 would not have had the same exposure to the resulting legislative amendments. This places greater emphasis on the need for stronger embedded process controls, as outlined below in this report.
- PRS has an ad-hoc induction training schedule.

3.11. During the 5 May Inspection, PRS advised that it conducts induction training for new staff within PRS, however, only once there is a sufficient number of inductees. This means that a newcomer may not receive formal induction training until several months after commencing within PRS. At the time of our 5 May Inspection, PRS induction did not specifically address metadata powers. However, we have been advised that since the breach, the AFP area outside of PRS that routinely processes metadata requests has delivered training at PRS induction.

3.12. We also suggest that the AFP implement a supplementary induction training package that PRS new-starters must complete, prior to being formally inducted into PRS if it is likely to be delayed. This supplementary training package should cover roles and responsibilities with regards to metadata, highlighting the higher thresholds for instances involving applications regarding journalists.

3.13. In light of the above, we make the following key recommendation:

> **Recommendation 1**
> 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*.

3.14. In response to this recommendation, the AFP advised that it is now finalising an online mandatory training package that all AFP authorised officers will need to undertake annually to maintain their authorised officer status. We will monitor the AFP's implementation of this recommendation, particularly in relation to how it assures itself that all authorised officers have completed the training. We will also monitor how the recommendation is applied to all staff involved in the exercise of metadata powers, not just authorised officers.

3.15. Subsequent to the 5 May Inspection, the AFP also advised that since the breach was identified, it has conducted a review of its training program and is in the process of arranging face-to-face training with regional offices to address the requirements relating to the exercise of metadata powers.

Personal accountability when exercising metadata powers

3.16. The AFP process for exercising metadata powers, like many other enforcement agencies, is split between a number of different staff. Generally, the process involves an applicant, an authorised officer, a person or team to liaise with the carrier regarding the request for disclosure, and any quality assurance roles.

3.17. During inspections, it is our practice to note the level of personal accountability that each officer of the agency demonstrates. Agencies that demonstrate high levels of personal accountability in the exercise of powers throughout all levels of staff, no matter what their involvement is in the process, are deemed as having a strong compliance culture.

3.18. In our metadata health check report, we noted that the AFP demonstrates a strong compliance culture, encouraging its officers to report compliance issues, maintaining a register of non-compliance and proactively disclosing compliance issues to our Office. In our opinion, this statement remains accurate.

3.19. During the 5 May Inspection, however, we noted that within PRS not all officers fully understood the legislative framework in which their functions formed a part. It was noted that the performance of this function was not a frequent nor substantive part of their duties, which therefore meant that fulfilment of that role in relation to metadata was very process based, without a broader

understanding of the legislative requirements including any recent legislative amendments.

3.20. At some other enforcement agencies, a broader understanding of the legislative framework among all staff involved in the exercise of metadata powers acts to increase the likelihood of errors and omissions being identified.

Process controls

3.21. During the metadata health check inspection, we noted that few of the AFP's controls for achieving compliance are automated and instead rely on the knowledge and experience of staff and embedded processes. Embedded processes may include things such as additional layers of quality assurance checks and the use of checklists and template documents.

3.22. Electronic system controls can ensure that applications that do not meet the required thresholds are automatically prevented from progressing. In the absence of automated electronic controls, embedded processes play a more significant role in achieving compliance.

3.23. In preparation for the Data Retention Act, the AFP prepared an additional checklist for authorised officers to refer to, which provided prompts regarding applications seeking to identify a journalist's source. Although this could have acted as an effective control against issuing the authorisations subject to the breach, as the use of the checklist was not mandatory, it was not used in these instances. In response to our suggestion during the health check inspection, the AFP advised that it would consider making this checklist mandatory for each authorisation. In light of this breach, the AFP should review the effectiveness and policy for use of the checklist by authorised officers.

3.24. Template documents are also an effective method of ensuring that relevant thresholds are met, and considerations are had, in an agency's exercise of metadata powers. In relying on the additional checklist for authorised officers, application and authorisation templates were not amended to reflect Journalist Information Warrant requirements.

3.25. During the 5 May Inspection, AFP staff were very receptive to stronger controls being embedded into template documents, to ensure compliance with s 180H of the TIA Act. As part of the AFP's response to the breach, it has updated its templates to incorporate a prompt regarding instances seeking to identify a journalist's information source, which will require an alternate process be undertaken. This prompt will act as a control on all authorisation applications submitted after the templates were updated.

3.26. Upon reviewing the new templates, and based on insight gained from oversight of other enforcement agencies, we suggest that the prompt be strengthened. As it currently stands, the prompt is specific to applications seeking to identify a journalist's source; however, we suggest that a broader range of scenarios is captured by the prompt, and that it be expanded to include any instance where it is reasonably believed that an application relates to a journalist. This will enable the AFP governance and legal areas to consider a wider range of scenarios and the need to obtain a Journalist Information Warrant in those instances.

3.27. The AFP also relies on a number of other controls to achieve legislative compliance, including a review mechanism that identifies deficiencies in metadata authorisations before they are provisioned on the carrier. In our view, this mechanism acts as a good control to prevent deficient authorisations from progressing, ensuring that, for example, the correct forms are used, that relevant offence thresholds have been met and that the authorised officer is not the same person as the requesting officer. The information collated through this mechanism may also inform future training activities.

3.28. We suggest that this mechanism be expanded to incorporate a check to ensure that any metadata authorisations relating to journalists have a corresponding Journalist Information Warrant.

Guidance documents

3.29. The health check inspection noted that the AFP has standard operating procedures on accessing telecommunications data, which are updated on an as needs basis and are available to anyone involved in the process of exercising metadata powers.

3.30. As part of the AFP's response to the breach, it has reviewed its standard operating procedures and other instructional materials to enhance guidance around Journalist Information Warrants. At the time of drafting this report, not all guidance material had been updated, and were still under review.

3.31. Included in these updates are the PRS-specific standard operating procedures. During the 5 May Inspection and subsequent activities, however, it was evident to our Office that not all staff within PRS were aware of the existence of a separate guidance document for PRS. Therefore, to ensure that all relevant guidance documents are referred to, the AFP should raise awareness within PRS that there is a PRS-specific guidance document, which addresses metadata powers.

3.32. We acknowledge, given the nature of the work of PRS, there may be sound reasons to have separate PRS-specific guidance documents. Combining the AFP-wide and PRS-specific guidance documents would remove any risk of inconsistencies between the two documents. Accordingly, the AFP may wish to reconsider the need for a separate document for PRS.

3.33. As the AFP intranet is likely to be referred to when applying for a metadata authorisation, the AFP should continue to review guidance material on its intranet to ensure that Journalist Information Warrant guidance is sufficiently prominent and unambiguous for all staff who infrequently, or may not have previously, exercised metadata powers. We note that the AFP immediately commenced this process upon identifying the breach and has already reviewed the guidance material that was referred to when attempting to ascertain whether the relevant authorisations were in breach of the TIA Act.

3.34. As part of this review, we also suggest that the AFP review its guidance and template documents to incorporate, where it may be assistive, prompts to refer to certain guidance and instructional materials.

3.35. The AFP can also issue authorisations for foreign law enforcement. There is guidance available in relation to issuing such authorisations, however, the only reference to the Journalist Information Warrant provisions appears to be in the authorised officer checklist, which notes that s 180H (2) of the TIA 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. We suggest that the AFP strengthen its controls to include the s 180H (2) prohibition throughout the foreign law enforcement guidance document and associated templates.

PART 4: CONCLUSIONS AND RECOMMENDATIONS

4.1. The Journalist Information Warrant provisions were introduced into the TIA Act to ensure that access to metadata 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 as a whole respects this higher threshold for journalists and takes its legislative obligations, particularly in relation to its use of covert and intrusive powers, seriously.

4.3. In any large, decentralised agency, there will inevitably be a risk that awareness raising does not reach every officer who is required to be in-the-know. In recognising this risk, all law enforcement agencies that can access metadata have implemented complementary measures to mitigate legislative non-compliance. Unfortunately, the complementary measures adopted by the AFP were not strong enough to prevent this breach from occurring.

4.4. There were four main actors which contributed to this breach:

- at the time of the breach, there was insufficient awareness surrounding Journalist Information Warrant requirements within PRS
- within PRS, a number of officers did not appear to fully appreciate their responsibilities when exercising metadata powers
- the AFP relied heavily on manual checks and corporate knowledge as it did not have in place strong system controls for preventing 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, they were not effective as a control to prevent this breach.

4.5. We accept that human error cannot be discounted in applying any legislation. To that extent we acknowledge that an agency's response to a mistake is more indicative of its compliance culture than the occurrence of that mistake.

4.6. In responding to this breach, we commend the AFP's voluntary disclosure to our Office and are satisfied that the AFP has adequately managed the unlawfully accessed data. In our view, the remedial measures already implemented by the time of the inspection go some way to ensuring that a breach of this nature does not recur. However, in light of the significant role that

the lack of awareness amongst a number of staff played in leading to this breach, we make the following key recommendation to the AFP:

> **Recommendation 1**
> 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*.

4.7. In response to this recommendation, the AFP advised that it is now finalising an online mandatory training package that all AFP authorised officers will need to undertake annually to maintain their authorised officer status. We will monitor the AFP's implementation of this recommendation, particularly in relation to how it assures itself that all authorised officers have completed the training. We will also monitor how the recommendation is applied to all staff involved in the exercise of metadata powers, not just authorised officers.

4.8. We also made a number of suggestions to the AFP regarding how it may strengthen its existing controls, as noted throughout the body of this report. In response to this, the AFP advised that it has already implemented some of these suggestions and will turn its attention to implementing all of them.

4.9. The Commonwealth Ombudsman has a statutory function to inspect the records of each enforcement agency to determine the extent of compliance with the legislative provisions regarding metadata by the agency and its officers. We conduct an inspection of each enforcement agency once each financial year, and report to the Commonwealth Attorney-General (the Minister) on an an annual basis. These reports must then be presented to both houses of the Parliament by the Minister.

4.10. Through the conduct of our routine annual inspections of the AFP, we will be monitoring the AFP's compliance under the TIA Act on an ongoing basis. At each of our inspections, we monitor progress on previous inspection findings at that agency. Therefore, the findings from this report will form part of the next routine metadata inspection to be conducted at the AFP during 2017-18, and will be reported to the Minister as soon as practicable after the end of 2017-18.

APPENDIX A: LEGISLATIVE BACKGROUND

The *Telecommunications (Interception and Access) Act 1979* (TIA Act) provides a legislative framework for agencies to lawfully receive information from telecommunication 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, metadata 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 metadata 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 telecommunication carriers to retain metadata for a minimum period of two years.

For agencies seeking to access metadata, 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 TIA Act by enforcement agencies.

Of particular note are the new requirements regarding Journalist Information Warrants under Division 4C, Chapter 4 of the TIA Act, which apply when an enforcement agency seeks to access the metadata 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 issuing an authorisation to obtain 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.[2]

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

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 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.[3]

Journalist Information Warrants are also subject to scrutiny from a Public Interest Advocate, who is appointed by the Prime Minister. Under the TIA 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.[4]

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.[5]

[3] Section 180T of the TIA Act stipulates the considerations that an issuing authority must be satisfied of when issuing a Journalist Information Warrant.
[4] Section 185D(5) details an agency's notification obligations in relation to Journalist Information Warrants.
[5] 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