COMMONWEALTH OMBUDSMAN

Australian Federal Police's (AFP) use and administration of telecommunications data powers 2010 to 2020

ACCESS TO IMMEDIATE RESPONSE LOCATION DATA UNDER THE *TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979*

April 2021

Report by the Commonwealth Ombudsman,
Michael Manthorpe PSM, under the *Ombudsman Act 1976*

REPORT NO. 03 | 2021

COMMONWEALTH OMBUDSMAN

CONTENTS

FOREWORD

This report is the outcome of my Office's own motion investigation into the Australian Federal Police's (AFP) use and administration of telecommunications data powers under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act). In particular, our investigation focussed on access to and use of one type of telecommunications data—location-based services (LBS), colloquially known as 'pings'.

My Office provides independent assurance that telecommunications data, including LBS, is only used in the circumstances permitted by the legislation and that agencies using these powers can demonstrate their compliance. We do this by inspecting a sample of records and reporting what we find each year. Our ability to provide this assurance is dependent on agencies providing full and accurate records of their use of the powers. As such, when the AFP identified records that showed ACT Policing (the AFP's community policing arm) had accessed LBS and that those records had not previously been provided to my Office, I decided it was appropriate for my Office to conduct its own investigation.

There were several important factors that informed my decision to commence an investigation, including:

- the covert and intrusive nature of this power
- the duration and potential scale of non-compliance with the TIA Act as a result of ACT Policing accessing telecommunications data outside the AFP's approved process
- the omission of the affected records from our Office's regular compliance inspections
- previous recommendations our Office has made to the AFP about non-compliance with the TIA Act.

The AFP identified records dating back to 2007 which showed ACT Policing accessed LBS outside the AFP's approved process. This meant two things:

- the access was not reported to the Minister for Home Affairs and the records were not provided to my Office, to be considered for inspection. My Office's inspections of the AFP's access to telecommunications data from 2015–16 occurred without full or accurate records to inform our assessment
- the risk of non-compliance with legislative requirements under the TIA Act was higher as the access occurred outside established processes approved by the AFP.

After identifying the records, the AFP did the right thing—they disclosed the issue to our Office and after discussion, commissioned PwC Australia (PwC) to conduct an internal audit of the affected records.

My Office's investigation focused on the scope and extent of any non-compliance, noting the potentially serious consequences, and the causes of any non-compliance, including culture, practices and procedures that contributed.

This report makes findings based upon the following themes:

- We identified that many of the authorisations made by ACT Policing for access to telecommunications data between 13 October 2015 and 2019 were not properly authorised. Of the 1,713 individual accesses to LBS by ACT Policing for that period, we were only able to provide assurance that nine were fully compliant with the TIA Act.

- Many LBS could have been accessed unlawfully which has a number of potential consequences. Firstly, if access was unlawful and the information relied on in prosecutions, there may be consequences for people convicted of an offence. While initial advice provided by the AFP to my Office was that the LBS obtained by ACT Policing was only used to locate someone to arrest them, we were unable to rule out the possibility that unlawfully obtained evidence, the LBS, may have been used for prosecutorial purposes. Secondly, the privacy of individuals may have been breached.

- We could not be satisfied that the scope of the breaches has been fully identified by the AFP nor the potential consequences and consider it is possible breaches have occurred in parts of the AFP other than ACT Policing.

- The AFP and ACT Policing missed a number of opportunities to identify and address that ACT Policing was accessing LBS outside the AFP's approved process earlier.

- The internal procedures at ACT Policing and a cavalier approach to exercising the powers resulted in a culture that did not promote compliance with the TIA Act. This contributed to the non-compliance identified in this report.

In response to PwC's report, the AFP made several changes to the way in which staff access prospective telecommunications data in an effort to improve compliance with the TIA Act. These have been useful first steps towards the AFP achieving future compliance. However, I consider the AFP needs to do more to confirm the extent of non-compliance with the legislation for this type of telecommunications data and remediate any consequences of non-compliance with the TIA Act identified in this report.

This report includes eight recommendations to assist the AFP in addressing these issues and implementing processes to prevent recurrence of similar issues.

Michael Manthorpe PSM
Commonwealth Ombudsman

PART 1: INTRODUCTION

1.1. Telecommunications data, also known as 'metadata', is information about a communication, but does not include the contents or substance of that communication. Examples of telecommunications data include, but are not limited to:

- subscriber information (for example, the name, date of birth and address of the person to whom the service is subscribed)
- the date, time and duration of a communication
- the phone number
- the location of a mobile device from which a communication was made (this may be requested at a single point in time or at regular intervals over a period)—this is LBS, the subject of this report.

1.2. Telecommunications data can be obtained from past records (historic telecommunications data) or from records on a real time ongoing basis (prospective telecommunications data). LBS data is prospective telecommunications data.

1.3. LBS is used by law enforcement to identify and locate persons of interest in investigating a crime. LBS is a useful investigative tool for law enforcement agencies and helps them to perform their functions.

1.4. The TIA Act sets out the requirements for lawfully accessing LBS. Unlike other intrusive powers which require agencies to obtain a warrant from an external authority, agencies can internally authorise a carrier to disclose telecommunications data.[1] However, before an authorised officer can do so, they must have regard to a range of considerations, including weighing the perceived utility and relevance of the telecommunications data to the investigation against the intrusion it will impose on the individual's privacy.

1.5. The authorisation is a record that the officer has made all the relevant considerations required under law. It can be supplemented by other records that show what the authorising officer considered. Amongst other things, the records of an LBS must show:

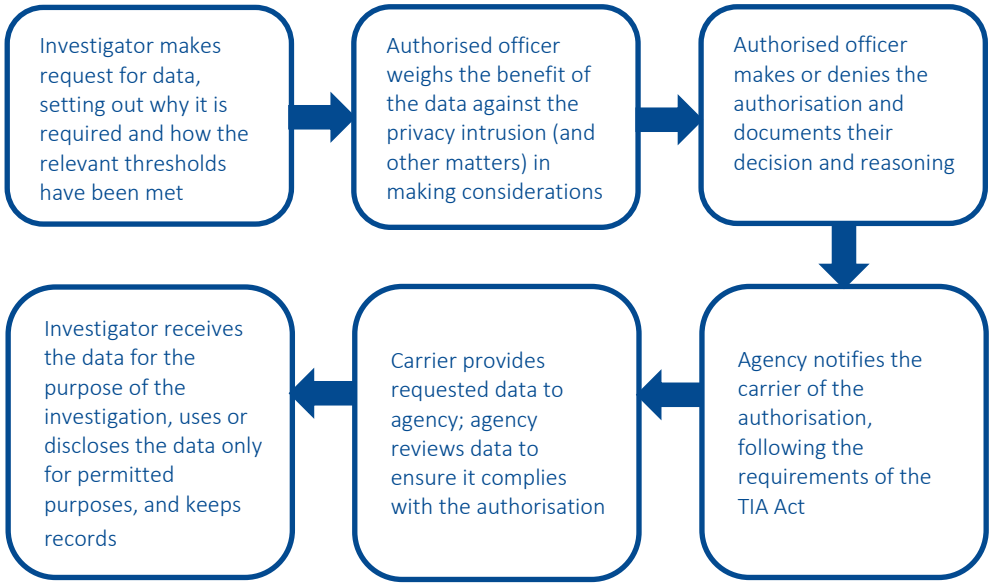
- who the authorising officer was
- that the authorising officer considered that the LBS was reasonably necessary for the investigation of a serious offence or an offence that is punishable by imprisonment for at least three years
- the need for the data was weighed against the privacy intrusion
- what was requested

[1] Except for requests to access telecommunications data of a journalist in order to identify a source, which may require an application for a journalist information warrant.

- the person that was the subject of the LBS and their connection to the offence being investigated.

1.6. The below figure demonstrates the typical workflow for authorising access to telecommunications data.

Figure 1—Typical authorisation process for disclosure of telecommunications data (excluding journalist information warrants)



The AFP's approved process for accessing prospective telecommunications data

1.7. The breaches in ACT Policing's access to telecommunications data arose, in part, due to ACT Policing not following the AFP's approved process when requesting and accessing prospective telecommunications data.

1.8. The AFP's approved process was that all requests for prospective telecommunications data, including LBS, must be made through the Covert Analysis and Assurance team (CAA), the AFP's centralised compliance team.[2] This centralised team also maintained record keeping for the purposes of reporting access to telecommunications data to the Minister and for inclusion in our Office's compliance inspections. Under this approved process all ACT Policing requests for prospective telecommunications data, including LBS, were required to be made through the AFP centralised compliance team.

[2] The area of the AFP now known as Covert Analysis and Assurance or CAA, was previously named the Telecommunications Interception Division or TID. For the purposes of this report, CAA or TID, depending on which name was in use at the time, will be referred to in this report as the AFP's centralised compliance team.

1.9. The AFP had approved a separate process for ACT Policing requesting historic telecommunications data (not LBS). Requests to access historic data by ACT Policing were made to a centralised team within ACT Policing itself. Importantly, this approved process did not extend to ACT Policing processing requests to access prospective telecommunications data (including LBS).

1.10. Throughout the course of our investigation, we identified several disparities in how this process had been communicated between the AFP's centralised compliance team and ACT Policing. This is discussed in more detail in Part 4 of this report.

Our Office's role in monitoring access to telecommunications data

1.11. Access to telecommunications data occurs covertly, which means the person to whom the data belongs is not aware of the access and cannot make a complaint if they think the action was unwarranted or unlawful. As a safeguard, since 13 October 2015 the TIA Act has required our Office to inspect and report on agencies' access to telecommunications data, to ensure it complies with the requirements of the TIA Act.

1.12. We conduct annual inspections of each agency that has accessed telecommunications data during the relevant period. Our inspections involve assessing a sample of records for access to telecommunications data. We look at the background material in the request, to check that the authorised officer had sufficient information available to them to consider the matters they must have regard to before authorising the disclosure of telecommunications data.

1.13. We also assess the processes agencies have in place to make authorisations, notify carriers and manage the data once it is received, in accordance with the legislative requirements of the TIA Act. By assessing a series of individual records in detail, alongside the processes, guidance and culture of an agency, we gain a detailed understanding of the agency's overall compliance with the TIA Act.

1.14. Under the TIA Act, agencies are obliged to report to the Minister for Home Affairs (the Minister) annually about the authorisations they made for the disclosure of telecommunications data and also make this information available to our Office for our inspections.

1.15. The Ombudsman reports the results of the Office's inspections and any resulting recommendations to the chief officer of the agency. We also prepare annual reports to the Minister about the results of our inspections of all agencies for the relevant period, which the Minister must table in Parliament. These reports hold agencies to account for their performance and we track their progress against our findings and recommendations at subsequent inspections.

Results of our previous inspections of the AFP's use of telecommunications data

1.16. We have made findings and recommendations about various aspects of the AFP's approach to accessing telecommunications data based on previous inspections. Those findings and recommendations were made without reference to the records the AFP disclosed in January 2020, because they were not included in data the AFP provided at the time of those inspections. However, in many instances, those findings and recommendations are directly relevant to the issues that appear to have caused ACT Policing to continue accessing prospective telecommunications data outside the AFP's usual process. These previous findings and recommendations are summarised in **Appendix B** of this report.

What happened in 2020

1.17. On 24 January 2020 the AFP disclosed to our Office that it had identified about 800 requests ACT Policing made for access to a certain type of prospective telecommunications data from 2007, outside the AFP's approved process. At that time the AFP could not be sure whether these authorisations had been made correctly and according to law or reported properly.

1.18. Following discussions with our Office about the disclosure, the AFP engaged PwC to conduct an internal audit, with the aim of establishing the scope of the affected records, identifying the root cause/s and recommending remedial action.

1.19. On 11 March 2020 the Ombudsman wrote to the AFP Commissioner Reece Kershaw, to advise he had decided to commence an own motion investigation into the AFP's management of telecommunications data. The investigation would be informed, in part, by PwC's report.

1.20. On 12 March 2020 ACT Policing issued a public statement[3] to acknowledge the issues affecting the identified records and advise that the AFP had commissioned an internal audit. On the same day the Ombudsman, Michael Manthorpe, issued a statement[4] to acknowledge the seriousness of the issues the AFP had disclosed and advise he had decided to commence an own motion investigation into the matter.

1.21. On 7 July 2020 the AFP Commissioner provided a copy of PwC's report to the Ombudsman.

[3] https://policenews.act.gov.au/news/media-releases/afp-scrutinise-telecommunications-requests

[4] https://www.ombudsman.gov.au/media-releases/media-release-documents/commonwealth-ombudsman/2020/12-march-2020-afp-disclosure-regarding-act-policings-access-to-telecommunications-data

PART 2: OUR INVESTIGATION

2.1. Our Office's role in monitoring the AFP's use of telecommunications data under the TIA Act is focused specifically on legislative compliance with Chapter 4 of the TIA Act. However, our Office has broad jurisdiction under the *Ombudsman Act 1976* (the Ombudsman Act) to investigate the administrative actions and decisions of Australian Government agencies, including the AFP, in response to a complaint or on the Ombudsman's 'own motion'.

2.2. In this instance we assessed that the seriousness and potential scope of the issues arising from the AFP's disclosure warranted an own motion investigation. An own motion investigation enables our Office to consider both the specifics of the AFP's compliance with the TIA Act and broader administrative issues, including the extent to which they contributed to identified legislative non-compliance. At the conclusion of an investigation, our Office can decide to publicly release a report with our findings.

Objective

2.3. The aim of our investigation was to:

- assess whether ACT Policing's access to LBS outside of the AFP's approved processes was compliant with the requirements of the TIA Act
- gauge the extent to which the AFP's approved processes had not been followed and how this contributed to any identified legislative non-compliance
- ascertain the level of assurance provided by the PwC audit and consider the comprehensiveness of the recommendations in its audit report
- inform additional recommendations to address systemic issues.

2.4. Our Office's investigation also sought to provide independent assurance that, following its disclosure, the AFP implemented appropriate administrative processes to comply with s 180(2) of the TIA Act. This involved:

- confirming it had identified the full scope of the issue, including whether ACT Policing was the only area of the AFP accessing prospective telecommunications data outside of the AFP's approved processes
- investigating any shortfalls in administrative arrangements that contributed to the breaches in record keeping, authorisation and reporting of prospective telecommunications data requests
- examining the effectiveness of the remedies the AFP put in place to prevent recurrence of similar issues
- highlighting the potential ramifications of non-compliance with the TIA Act, including how the data was used.

Scope and methodology

2.5. Our methodology comprised four components:

- assessment of the AFP's compliance based on review of the affected records
- reviews of procedures and other guidance material relied on by the AFP during the relevant period
- interviews with staff at the AFP and ACT Policing
- reviews of emails dated between 2010 and 2020 relevant to the AFP and ACT Policing's awareness of, and response to breaches in the use of telecommunications data.

2.6. Our assessments and findings were also informed by previous recommendations our Office has made to the AFP as a result of our regular and ad-hoc compliance inspections.

Assessment of records

2.7. Our inspection criteria were broken down as follows:

1. Is the agency only dealing with lawfully obtained telecommunications data?

    1.1 Were authorisations for telecommunications data properly applied for, given and revoked in accordance with legislation?

    1.2 Did the agency identify any telecommunications data that was not within the parameters of the authorisation?

2. Has the agency properly managed telecommunications data?

3. Has the agency complied with journalist information warrant provisions?

    3.1 Does the agency have effective procedures and controls to ensure that it is able to identify the circumstances in which a journalist information warrant is required?

    3.2 Did the agency properly apply for journalist information warrants?

    3.3 Did the agency notify the Ombudsman of any journalist information warrants?

    3.4 Did the agency revoke journalist information warrants when required?

4. Has the agency satisfied certain record keeping obligations?

5. Does the agency have a culture of compliance?

2.8. Our assessments during the investigation also emphasised the following, which are crucial subcomponents of our regular inspections criteria:

- The availability of sufficient information to enable an authorised officer to be reasonably satisfied that any privacy intrusion caused by the disclosure of telecommunications data is justified in line with s 180F of the TIA Act.

- Authorised officers personally had regard to the considerations about privacy under s 180F and limits under s 180(4), and kept records to demonstrate the authorisation was properly made, including whether the authorised officer took into account the considerations required by s 186A(1)(a)(i) of the TIA Act.

- Authorised officers demonstrated they had regard to the journalist information warrant considerations in line with s 180H of the TIA Act.

2.9. It is important to note that our assessments were limited to those records the AFP made available.

Interviews and document review

2.10. In addition to the records-based assessments, we met with AFP and ACT Policing staff on several occasions to identify factors that may have contributed to the non-compliance. This included discussions with members of the AFP and ACT Policing who were initially involved in identifying the issue, members who scoped the extent of the issue, and members who amended processes to prevent recurrence.

2.11. We also spoke with members of ACT Policing who were involved in processing the affected authorisations, and with authorised officers who approved a large number of the authorisations to access telecommunications data outside the AFP's approved processes.

2.12. Given the lack of contemporaneous records to demonstrate point-in-time processes, practices and guidance materials, we asked the AFP to search for relevant emails and corporate records covering the period of the affected records, from 2010 to 2020. We selected emails to be reviewed from the search results, based on key terms and the names of personnel relevant to the investigation.

2.13. The Secure Electronic Disclosure Node, or SEDNode, is an online portal through which law enforcement agencies may submit requests for data from telecommunications providers. Most of the requests for LBS made by ACT Policing were submitted via SEDNode. We therefore also obtained, and inspected invoices detailing the AFP's use of SEDNode for the period from 2010 to 2020, to cover gaps we identified in data the AFP had exported from SEDNode.

PART 3: COMPLIANCE FINDINGS

Extent of access to telecommunications data outside AFP approved processes

3.1. It is important to determine the extent of access to telecommunications data outside of AFP approved processes by both ACT Policing and any other area of the AFP noting that any such access to telecommunications data has an enhanced risk of non-compliance with legislative requirements under the TIA Act. Any such access has also not been subject to our Office's oversight.

3.2. Our Office could not be satisfied the AFP had identified the full extent of accesses to telecommunications data outside AFP approved processes. The extent of ACT Policing's usage could not be verified, and we consider it is possible there was non-compliance in other parts of the AFP.

3.3. SEDNode was a key source of information for our investigation and PwC also used it to identify the number of times ACT Policing had accessed LBS. However, there are some caveats that apply to this data which may impact its reliability and comprehensiveness. In particular, the data only extends back to 2013 and only one member of ACT Policing could access all requests, which means the search could not be replicated by another user to check the same results were returned.

3.4. The AFP did not independently verify the completeness or accuracy of the ACT Policing SEDNode data. However, the AFP sought an assurance, via regional chains of command, that other areas of the AFP were not accessing prospective telecommunications data, including LBS, outside the AFP's approved process. However, it did not appear to have verified that these assurances were accurate which was needed given the movement of personnel and the extensive period over which SEDNode has been in use at the AFP.

3.5. Noting the technical challenges of accessing the data, we asked the AFP to provide our Office with data for all SEDNode requests it made since 13 October 2015, to enable our Office to independently assess the nature of the requests and determine whether there was non-compliance in other areas of the AFP during the period of our oversight.

3.6. At the time of finalising our report, the AFP advised it was in the process of obtaining administrator-level SEDNode data to access records from November 2017. Limitations to access certificates mean administrator access only extends to November 2017. Access by individual AFP members would extend back further, if security certificates for previous periods have been retained.

3.7. To further assist us to independently assess whether, and to what extent the AFP's regional commands had followed the required processes, we asked the AFP to provide us with invoices from the vendor of SEDNode. The AFP was able to provide itemised invoices for the period from December 2011 to October 2020 but, due to an invoicing change, the invoices from December 2017 onwards did not itemise LBS charges.[5] As a result, we could

[5] SEDNode is used for a number of checks, not only LBS 'pings'. From December 2017 these other checks were itemised on invoices, but LBS 'pings' were not.

not fully assess the AFP's use of LBS functionality between December 2017 and October 2020.

3.8. Despite not being comprehensive, the invoices showed that between 2012 and 2016, other areas of the AFP had used the LBS functionality in SEDNode. We identified that, in addition to ACT Policing, three other areas had been billed for LBS. These were:

- AFP Telecommunications Interception Division (now known as Covert Analysis and Assurance)[6]
- AFP Operations Coordination Centre (now known as National Operations Support Centre)
- AFP Adelaide.

3.9. AFP advised some of this access had occurred under s 287 of the *Telecommunications Act 1997*, which provides for access to telecommunications data in life-threatening situations. However, due to a lack of available information to verify the basis for the LBS searches and references in historical guidance documents to other regions accessing LBS through SEDNode, we could not exclude the possibility that some of these searches were undertaken under the TIA Act outside the AFP's approved processes, and that telecommunications data could have been accessed unlawfully.

3.10. Based on our inspection of its records, ACT Policing appeared to operate incorrectly, on the basis that instances where the LBS was unsuccessful, such as where a phone was switched off or was not subscribed to the relevant provider, did not require an authorisation. For example, in one instance, officers prepared a retrospective approval to cover 17 individual accesses to LBS, despite there being 20 individual accesses, three of which were unsuccessful.

3.11. In light of this approach, we cannot be confident that the AFP's available records of authorisations made reflect all accesses to LBS. Comparing the SEDNode data to the authorisations, we identified accesses to LBS which we were unable to link to any authorisation. We consider it is likely this includes instances where a mobile phone was switched off or the service was not subscribed to the relevant provider.

3.12. Ultimately, our Office cannot provide assurance that the AFP has accounted, or is able to account, for all LBS conducted at ACT Policing and other areas of the AFP. Given the lack of comprehensive data and noting that, until recently, members outside of the AFP's centralised compliance team had access to SEDNode, we consider it is unlikely that all occurrences outside of the AFP's usual process have been identified. However, the business requirements of ACT Policing differ substantially from those of the broader AFP and make ACT Policing more likely to use LBS than other areas. While this has not been tested in other areas of the AFP, we consider it is unlikely that, if other use has occurred, it is as extensive as that at ACT Policing.

3.13. Nevertheless, it is important that the AFP undertakes all necessary measures to identify the full extent and scope of LBS access that occurred outside of the AFP's approved

[6] These were included in the AFP's reporting to the Minister

procedures and identify any instances where this may have resulted in unauthorised access to telecommunications data due to non-compliance with the TIA Act.

3.14. Given that we are unable to determine the scope of this issue, we recommend that:

Recommendation 1

To ascertain whether other areas of the Australian Federal Police (AFP) have accessed LBS, the AFP should obtain and audit all data from SEDNode for all users, to the extent that data is available, to determine the number of requests made for LBS, covering the period from 13 October 2015 to 31 January 2020.

The AFP should also continue to monitor the use of SEDNode nationally, to ensure that business areas access appropriate request types in line with their designated roles.

Recommendation 2

The AFP include any LBS authorisations made outside ACT Policing between 13 October 2015 and 31 January 2020 in records for our Office's next inspection of the AFP's compliance with Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*.

Level of assurance provided by PwC's compliance audit

3.15. Our investigation identified substantial variations between the levels of non-compliance identified by PwC in its internal audit and those resulting from our records-based assessments.

3.16. Our review of PwC's materials identified that its audit did not address all areas we consider are fundamental to assessing an agency's compliance when accessing telecommunications data under the TIA Act. In our view the consequence of this was that its recommendations to the AFP and ACT Policing were not sufficient to address the range of issues that contributed to the non-compliance.

3.17. In contrast to PwC we assessed:

- the privacy consideration requirements of s 180F of the TIA Act and record-keeping requirements that indicate whether privacy considerations were made in line with s 186A(1)(a)(i) of the TIA Act
- consideration of the journalist information warrant requirements of s 180H of the TIA Act
- whether the service number authorised was the service notified to the carrier i.e. that the correct service was the subject of the LBS.

3.18. Due to the different approaches to determining compliance, our investigation identified a significantly higher rate of legislative non-compliance than PwC's audit.

Assessment of records to determine extent of compliance

3.19. We conducted assessments on two sets of records. *Record Set A* covered authorisations that were made and the LBS that was accessed following the commencement of our oversight on 13 October 2015 until 3 January 2020. *Record Set B* covered authorisations made prior to the commencement of our oversight on 13 October 2015 and the correlating instances where ACT Policing had accessed LBS.

Assessment of ACT Policing authorisations and SEDNode data—Record Set A—13 October 2015 to 3 January 2020

3.20. Based on the records the AFP provided, we identified 135 authorisations ACT Policing made for prospective telecommunications data on or after 13 October 2015. We completed comprehensive compliance checks of these records, with an emphasis on records supporting the reason for approval of access to telecommunications data and privacy considerations as required by the TIA Act.

3.21. Our compliance checks found that the majority of access to LBS by ACT Policing during this period outside of AFP approved processes, were also non-compliant with the TIA Act. Of the 135 authorisations for access to prospective telecommunications data assessed in Record Set A, every authorisation was affected by at least one of the compliance issues discussed below.

3.22. The types of compliance issues we identified in our assessments of authorisations ranged in seriousness. For example, we identified instances of significant non-compliance that may affect the lawfulness of the LBS accessed by ACT Policing, such as where LBS was accessed before a written authorisation was in place. We also identified less serious compliance issues that, whilst not strictly compliant with the TIA Act, are less likely to affect the lawfulness of the accessed LBS, for instance, where the short particulars of the offence were not stated on the authorisation as required by s 12(1)(h) of the Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2018.

3.23. The table below provides the results of our compliance assessments of ACT Policing's prospective authorisations for LBS between 13 October 2015 and 3 January 2020.

Compliance issue	**Number of affected authorisations**
No record of information put before the authorised officer to support determination of authorisation.	119 of 135
No record of privacy considerations by authorised officer.	112 of 135
Insufficient record of information put before the authorised officer to support determination of authorisation.	16 of 135

No record of information to indicate journalist information warrant considerations had been made.	123 of 135
Journalist information warrant considerations made only in respect of the need for a warrant; not whether the request for telecommunications data related to a journalist.	12 of 135
Authorisation made after carrier notified.	14 of 135
Unable to determine whether authorisation was made before LBS accessed.	103 of 135
Authorisations assessed as compliant	**0**
Authorisations assessed as non-compliant	**135**

NOTE: an authorisation may have been affected by more than one compliance issue. For example, there may not have been any record of information put before the authorised officer to support determination of authorisation as well as no record of the privacy considerations made by the authorised officer.

Authorised officer considerations not demonstrated

3.24. Under s 180F of the TIA Act, before making an authorisation for access to telecommunications data, an authorised officer must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use of the telecommunications data is justifiable and proportionate, having regard to certain matters covering the:

- gravity of the conduct being investigated
- relevance and usefulness of the telecommunications data
- reason why the disclosure is proposed.

3.25. Section 186A(1)(a)(i) of the TIA Act requires the chief officer of an agency to ensure documents or other materials are kept that indicate whether an authorisation was properly made, including whether all relevant considerations have been taken into account.

3.26. Our Office does not assess the merits of authorisations. Rather, our assessments focus on whether authorised officers were provided with enough information to appropriately consider the requirements under s 180F of the TIA Act and all other relevant considerations.

3.27. Based on our assessment of Record Set A, we were not satisfied the AFP had demonstrated that authorised officers consistently had regard to the required considerations under the TIA Act.

3.28. We found that, generally, authorised officers did not record the considerations underpinning their decision. In 119 of the 135 authorisations in Record Set A, there was no application for access to telecommunications data. The application would normally provide

the authorised officer with information that they use to satisfy themselves that the authorisation can be made in accordance with the legislation. In the remaining 16 records there was limited, or no background information provided in support of the application that would enable the authorising officer to have regard to the privacy considerations.

3.29. Of the authorisations that did contain reference to the privacy considerations, these generally consisted of template wording, and in some cases, this was incomplete. We do not consider template wording always sufficiently demonstrates the privacy considerations each authorised officer made under s 180F of the TIA Act.

3.30. Our assessments also identified that records generally contained very limited information to establish a connection between the offence being investigated and the proposed authorisation, or to explain how the person of interest was linked to the service for the proposed authorisation. In the absence of this information it was not clear how the authorised officer could make the necessary privacy considerations in relation to the subscriber of the service and the value of the evidence to the investigation.

3.31. The same issues are included in several of our previous compliance inspections of the AFP's use of telecommunications data. We regularly emphasise the critical role of the authorised officer as a control for ensuring telecommunications data powers are used appropriately, and the importance of capturing the information that an authorised officer had regard to when making an authorisation.

3.32. The sorts of records we would expect to see to demonstrate that the required considerations have been made include details of a verbal briefing by an investigator to inform the authorised officer's understanding or records that detail what the authorised officer considered.

Journalist information warrant considerations

3.33. Section 180H of the TIA Act states that an authorised officer must not make an authorisation that would authorise the disclosure of information or documents of a particular person if:

(1) the authorised officer knows or reasonably believes that particular person to be a journalist or an employer of a journalist, and

(2) a purpose of 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 (JIW) is in force.

3.34. These provisions were introduced into the TIA Act in October 2015 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 and are subject to additional scrutiny.

3.35. Of the 135 authorisations in Record Set A, 123 did not include any information to indicate JIW considerations had been made, which is a requirement under the TIA Act. This reflects a limited appreciation for the requirements of the TIA Act.

3.36. In the remaining 12 records, JIW considerations had only been made in respect of the need for a warrant; not whether the request for telecommunications data related to a journalist.

3.37. Use of telecommunications data to identify a journalist's source is uncommon and there is no evidence to indicate that any of the LBS accessed by ACT Policing was used to identify a journalist's source. However, given the specific provisions relating to journalists under the TIA Act, we consider that agencies should actively demonstrate how they have considered and complied with s 180H of the TIA Act to determine whether a journalist information warrant is required before making an authorisation for the disclosure of telecommunications data. In the 123 authorisations we assessed that did not include any information to indicate JIW considerations had been made, we were not satisfied this had occurred and so cannot provide assurance the LBS accessed by ACT Policing was not used for this purpose. These issues have been identified in previous inspections of the AFP's use of historic and prospective telecommunications data authorisations.

Requirement for authorisations for access to prospective telecommunications data to be made prior to the carrier being notified

3.38. Under s 180(2) of the TIA Act, a criminal law-enforcement agency such as the AFP can only access telecommunications data if an authorised officer has authorised the disclosure of specified information or documents that come into existence while an authorisation is in force. This means a formal written authorisation must be in place before a request is sent to the carrier seeking telecommunications data.

3.39. Although the TIA Act does not require that authorisations are time stamped, where there is no indication of the time at which an authorisation was made and the authorisation is sent to the carrier on the same date, it is unclear whether the authorisation was in place prior to notification of the authorisation being sent and, in turn, whether the telecommunications data was lawfully disclosed.

3.40. Based on our review of ACT Policing Intelligence's Standard Operating Procedures (SOPs), it was an accepted practice to seek retrospective authorisations for access to LBS.

3.41. For 103 authorisations in Record Set A, it was unclear whether the authorisation was made before the LBS was accessed. In a further 14 instances, the authorisation appeared to have been made after the authorisation was notified to the carrier.

Compliance assessment of LBS accessed through SEDNode in Record Set A

3.42. Multiple instances of access to LBS may be provided under a single authorisation, depending on the scope of what has been authorised. Based on the records the AFP provided, we identified 1,713 instances of access to LBS between 13 October 2015 and 3 January 2020.

3.43. We were able to correlate the 135 authorisations in Record Set A to 1,301 instances where ACT Policing had accessed LBS using SEDNode and eight instances where LBS had been provided outside of SEDNode. However, we were unable to find a linkage between the remaining 412 instances and an authorisation, which casts doubt on their legality. With

respect to all instances, we could confirm that only nine instances were compliant[7] 91 instances were non-compliant and for 1,613 instances we were unable to determine compliance.

3.44. Common compliance issues that we identified in our assessment of the accessed LBS include: LBS accessed on an incorrect service number, LBS accessed after an authorisation expired, additional LBS accessed that was not authorised, no time specified on an authorisation and authorisations that were not signed. More detail about each of these issues is set out below.

3.45. The following table presents our compliance assessments of the individual instances ACT Policing accessed LBS through the SEDNode tool between 13 October 2015 and January 2020, based on the SEDNode data provided to our Office.

Compliance issue/ assessment	**Number of instances of LBS accessed through SEDNode affected**
LBS accessed prior to written authorisation	57
LBS accessed on incorrect service number	10
LBS accessed after authorisation expired	1
Additional LBS accessed that was not authorised	4
General non-compliance due to signature or authorisation issue	5
No record to correlate notification to LBS	4
No time specified on authorisation	10
Total instances of LBS assessed as compliant	**9**
Total instances of LBS assessed as non-compliant	**91**
Records (notification) not available to correlate SEDNode data to authorisation	125
Unable to determine whether authorisation preceded LBS access—no time specified on authorisation	1,048
Combination of above—no record of LBS access and no time specified on authorisation	28

[7] Compliance in this context is strictly in respect of the LBS complying with the parameters of the authorisation and there being a written authorisation in place prior to the LBS being accessed. It does not include other types of non-compliance issues, which are discussed above.

Total instances of LBS accessed where we were unable to determine compliance	**1,201**
No authorisation or notification to correlate to accessed LBS	410
LBS not accessed under the TIA Act (instead LBS accessed under s 287 of the *Telecommunications Act 1997*)	2
Total instances of LBS accessed where we were unable to determine compliance as LBS was unable to be correlated to an authorisation	412
Total	**1,713**

Assessment of ACT Policing SEDNode Data—Record Set B—2009 to 12 October 2015

3.46. Our review of records prior to 13 October 2015 did not involve an assessment against our usual comprehensive methodology but, rather, was intended to identify any significant compliance issues against a limited criteria. This informed our understanding of the evolution of practices and scope of significant compliance issues at ACT Policing from 2009 to 12 October 2015 (Record Set B).

3.47. The issues identified in Record Set B corresponded to the procedural issues identified in the selected emails covering the period of the affected records, that we reviewed and are discussed further in Part 4 of this report. These issues include authorised officers actively encouraging requesting officers not to delay accessing LBS, processing requests to telecommunications carriers prior to authorised officers making an authorisation, and an extensive practice of retrospective approval of authorisations.

3.48. For authorisations made prior to 13 October 2015, we identified 155 compliance issues over approximately 665 available authorisations. We did not, as we did with Record Set A, assess any data accessed under these authorisations, or attempt to correlate these authorisations with the SEDNode data. Had we done so, further compliance issues may have been identified.

Issue	**Authorisations affected**
Serious legislative compliance issues	
Authorisation made after access to LBS had occurred (ss 180(1) and (2), 183 TIA Act)	90
Authorisation not signed, access to LBS occurred (ss 180(1) and (2), s 183 TIA Act and s 12(2) of the Determination)	15

Unable to determine whether record represents original or true authorisation (ss 186A(1)(a) and 186A(1)(a)(i) TIA Act)	3
Authorisation exceeds the permitted 45 days (s 180(6)(b)(i) TIA Act)	1
Service authorised not stated on authorisation (s 180(1)-(2) TIA Act and s 12(1)(g) of the Determination)	1
Offence threshold of three years not met (s 186(4) TIA Act)	1
Retrospective approval and advice that authorisation should have proceeded without approval regardless (ss 180(1) and (2), 183 TIA Act)	1
Other legislative compliance issues	
For ACT offences, authorisation states it is an offence against a law of the Commonwealth or a state rather than a territory (s 186A(1)(a)(i) TIA Act and s 12(1)(h) of the Determination in relation to short particulars of the offence)	17
Short particulars of offence not stated (s 186A(1)(a)(i) TIA Act and s 12(1)(h) of the Determination in relation to short particulars of the offence)	3
Offence incorrectly stated (s 186A(1)(a)(i) TIA Act and s 12(1)(h) of the Determination in relation to short particulars of the offence)	7

3.49. As discussed in our compliance findings for Records Set A, we identified a lack of information to substantiate requests for access to LBS.

Potential consequences of non-compliance with the TIA Act

Use and disclosure of accessed LBS

3.50. Section 186A(1)(g) of the TIA Act sets out an agency's obligations to keep records relating to the use and disclosure of information obtained under a telecommunications data authorisation to show that any use or disclosure occurred in circumstances permitted by the TIA Act.

3.51. Of the 135 authorisations in Record Set A, we did not identify any records to demonstrate how the accessed LBS had been used or disclosed. It is important that such records are made, so that an agency may undertake appropriate actions if access to that information is later determined to be invalid.

3.52. We were concerned by the AFP's inability to account for how LBS or prospective telecommunications data information, which may have been obtained unlawfully, had been used. While the AFP advised its practice was to only access LBS for operational reasons (for example, locating an individual in order to arrest them) rather than to gather evidence, we were unable to discount the possibility that such information could have contributed to, or had a bearing on, prosecutorial and evidentiary matters. The consequence of a prosecution relying on unlawfully obtained LBS could be very serious.

3.53. Due to the high risk associated with this possibility, the lack of such records and the extensive compliance issues identified in our records based assessments, we make the following recommendation:

Recommendation 3

The Australian Federal Police (AFP) should seek legal advice on any implications arising from accessing prospective telecommunications data that has not been properly authorised.

A) Where it has been identified that prospective telecommunications data has been accessed without the proper authorisation, or where the AFP is unable to determine that the authorisation complied with legislative requirements, an assessment should be made by the AFP to determine whether the prospective telecommunications data has been used for any evidential or prosecutorial purposes.

B) Where the AFP has determined that unauthorised prospective telecommunications data has been used for evidential or prosecutorial purposes, legal advice should be sought by the AFP to assess any implications of each individual use of the unauthorised prospective telecommunications data.

C) The AFP should quarantine all records where a written authorisation was not in place before prospective telecommunications data was accessed until after our Office's 2021–22 inspection of the AFP's compliance with Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*, after which time the unauthorised data should be destroyed.

Reporting to the Minister about use of telecommunications data

3.54. Ministerial reporting under s 186 of the TIA Act provides an important transparency mechanism by telling the public how extensively certain powers are used by agencies. As an internally authorised power, prior to 13 October 2015, this reporting was the sole public transparency mechanism for the telecommunications data regime.

3.55. From 2010 to 2018, ACT Policing provided copies of its authorisations for prospective telecommunications data, including LBS, to the AFP for inclusion in Ministerial reporting. We sought to confirm whether these authorisations had been included in the AFP's reports to the Minister under s 186 of the TIA Act about its use of telecommunications data powers. This involved comparing the figures in the Ministerial reports with the figures for prospective authorisations processed by the AFP's centralised compliance team.

3.56. We also reviewed the AFP's working documents for calculating the figures to ascertain how the AFP determined the total number of prospective telecommunications data authorisations each year. We then compared any substantial variance between these figures against the available records from ACT Policing, which informed our view about whether its authorisations for LBS had been reported to the Minister.

3.57. We compared reporting for the following years, where information was available, and indicated where ACT Policing authorisations were reported to the Minister.

Reporting year	AFP internal figures for s 180 authorisations	ACT Policing LBS authorisations reported to the AFP	Total s 180 authorisations in report	ACT records reported to the Minister
2009–10	148	65	148	No, removed in an AFP quality assurance process
2010–11	169	215	683[8]	Yes
2011–12	487	127	487	No, removed in an AFP quality assurance process
2012–13	683	77 records provided as part of this investigation	683	No
2013–14[9]	956	100 records provided as part of this investigation	1037	Unable to confirm
2014–15	1623	105 records provided as part of this investigation	1624	No

[8] Working calculations by the AFP centralised compliance team reflected 383 authorisations, we were unable to locate information to account for the additional 300 authorisations reported.

[9] It is possible that ACT Policing's LBS authorisations were included for this reported year; however, without working documents we were unable to definitively account for the difference of 81 authorisations, despite it roughly aligning with ACT Policing known figures of 100 authorisations for 2013–14.

Reporting year	AFP internal figures for s 180 authorisations	ACT Policing LBS authorisations reported to the AFP	Total s 180 authorisations in report	ACT records reported to the Minister
2015–16	2591	62 records provided as part of this investigation	2592	No
2016–17	3045	34 records provided as part of this investigation	3045[10]	No
2017–18	3701	38 provided as part of this investigation	3701	No
2018–19	4707	17 records provided as part of this investigation	4707[11]	No

3.58. Our analysis led us to conclude that, in most instances during the relevant period, ACT Policing's access to LBS was not included in AFP's reporting to the Minister under the TIA Act.

3.59. At least between 2009–10 and 2011–12, ACT Policing provided monthly reports to the AFP about its authorisations. Working documents which we reviewed indicated that, in several years, the AFP's centralised compliance team made reference to additional authorisations but ultimately excluded these from the total number reported to the Minister.

3.60. AFP records also indicated that, until 2018, ACT Policing continued to send its hardcopy authorisations to the AFP's centralised compliance team.

3.61. It was not clear why the AFP excluded the data ACT Policing provided, or why the regular receipt of data and hard copy records did not cause the AFP to query why ACT Policing was accessing LBS outside the AFP's approved processes.

3.62. To address the omission of authorisations for prospective telecommunications data made by ACT Policing in reporting to the Minister for Home Affairs, as required under s 186 of the TIA Act, we make the following recommendation:

Recommendation 4

The Australian Federal Police should revise its reporting of all authorisations for prospective telecommunications data under s 186 of the *Telecommunications (Interception and Access)*

[10] In our inspection report for the 2016–17 period we recorded 3,107 prospective telecommunications data authorisations records were made available. This appears to have been a typographical error.

[11] In our inspection report for the 2018–19 period we recorded 4,711 prospective telecommunications data authorisations records were made available.

Act 1979 to the Minister for Home Affairs between 1 January 2009 and 30 June 2020 to ensure all authorisations for access to prospective telecommunications data have been included and provide addendums to the Minister for Home Affairs, as required.

PART 4: WHAT CONTRIBUTED TO THE NON-COMPLIANCE?

4.1. As part of our Office's investigation, we considered broader administrative issues to examine the extent they contributed to the identified legislative non-compliance and inform additional recommendations, addressing any other systemic issues that might give rise to similar instances of non-compliance in future.

4.2. Our Office's investigation showed a continued and long-standing cavalier attitude to the requirements under the TIA Act for the lawful authorisation for disclosure of LBS, despite isolated attempts to improve practices over the years.

4.3. The following issues appear to have contributed to the non-compliance:

- a loss of corporate knowledge
- a lack of consistent processes and procedures
- a lack of engagement between ACT Policing and the AFP's centralised compliance team
- a lack of awareness of approved procedures
- the failure to question accepted practices
- a lack of appreciation of the serious nature of the intrusiveness of these powers.

Procedural issues affecting ACT Policing's access to telecommunications data

ACT Policing's documented procedures

4.4. Based on emails we reviewed, we were able to determine that, from 2010, ACT Policing established internal governance, independent of the AFP's own, for accessing LBS. Our review of these governance materials indicated that ACT Policing did not have a high level of appreciation for the TIA Act's requirements and that some of its standard processes, set out in its guidelines, were contrary to the TIA Act.

4.5. We also determined that ACT Policing had documented practices in place to provide its LBS forms to the AFP's centralised compliance team as late as October 2017 (the practice persisted into 2018 even after the process was removed from the documents). This accounts for the AFP's centralised compliance team being in possession of large numbers of ACT Policing's hardcopy authorisations. It is not clear why ACT Policing ceased providing these records to the AFP's centralised compliance team in 2018 or why the AFP did not note that these records were no longer being received.

4.6. From 2010 to 2020, internal correspondence between ACT Policing Intelligence members indicated ACT Policing was grappling with ongoing compliance issues, particularly members conducting telecommunications data searches without approval.

4.7. During our interviews with ACT Policing members, they advised that ACT Policing did not have specific SOPs that governed the LBS process and, instead, staff relied on corporate knowledge and ad hoc guidance provided via email.

4.8. However our email audit identified that, until at least 1 October 2015, ACT Policing maintained a specific SOP on 'triangulations' (LBS) on the AFP's repository known as SPOKES, as well as a specific template it had developed for these authorisations. Further, as recently

as December 2016 ACT Policing had guidance material that referenced ACT Policing undertaking 'pings' and its training material also continued to reference the ACT Policing's ability to internally access LBS.

4.9. Notwithstanding the problems with ACT Policing's approach to accessing LBS, these records make it clear the procedures were long-standing, well-established and clearly communicated to those within the business area.

ACT Policing's approach to compliance

4.10. During our review of emails, we identified numerous internal communications that highlighted significant problems affecting ACT Policing's use of LBS and others that demonstrated ACT Policing's efforts to improve its practices and standards. Despite ACT Policing's regular engagement with intelligence staff and investigators on issues relating to LBS practices, there appears to have been little improvement in the quality of processes ACT Policing employed from 2010 to 2020.

4.11. From October 2015 onwards, ACT Policing regularly communicated with relevant staff about the need to provide sufficient information to justify a request for access to telecommunications data. This is an important juncture as it followed the implementation of the revised telecommunications data regime. However, in addressing these amendments, it appeared that ACT Policing had largely focussed on the process of supplying information to justify a request, without considering whether its current process as a whole was compliant. For example, records show that the practice of retrospectively completing authorisation documentation was common until 2020.

4.12. Some emails indicate that both requesting and authorising officers had a limited understanding of their obligations when applying for and authorising access to telecommunications data. The emails show ACT Policing often took an informal approach to using these intrusive powers. This informality occurred despite senior staff sending email reminders to broad distribution lists to remind requesting and authorising officers that access to LBS should be considered and undertaken only when absolutely necessary.

4.13. Below is a summary of relevant emails we identified during our audit of emails sent between 2010 and 2020. These provide important context to the compliance findings that are set out in Part 3 of this report. These emails reflect the widespread nature of the procedural and cultural issues affecting ACT Policing's compliance in relation to accessing LBS.

4.14. These emails refer to LBS searches that occurred without approval, use of LBS without an apparent connection between the phone to be located and the offence, and instances where there was a lack of clear justification for the need to undertake LBS searches.

4.15. On some occasions authorised officers approved LBS searches within minutes of receiving a request and there is no documentation available that reflects they had sufficient information to properly consider the circumstances of the request. It is important to note that approval via email does not always constitute an authorisation to access telecommunication data, as an authorisation must meet a number of requirements.

2010–2013

- On 13 October 2010, a senior officer in ACT Policing advised that they had misplaced their mobile phone and had a staff member 'ping' the phone in case it had been stolen.

- On 1 January 2012, a member of ACT Policing and an investigator discussed obtaining LBS to identify a person of interest. It then appears that an LBS was undertaken on a mobile phone number, despite it being unclear to both members as to whether the person of interest still used that phone number. An email states 'Most recent linked mobile is [redacted] Who knows if [redacted] still has that mobile though???'

- On the morning of 8 May 2012, following a request the previous afternoon to approve access to LBS, the authorised officer advised the requesting member 'Hope this proceeded without my approval'.

- On 10 May 2013, ACT Policing Intelligence and investigators discussed strategies for identifying a person of interest. Due to the costs associated with an after-hours 'ping' on the person of interest's phone (which was with a carrier that could not be 'pinged' through SEDNode), ACT Policing appears to have decided to access LBS for the person of interest's girlfriend, in the apparent hope that the person of interest was co-located with his girlfriend. Information in this chain of emails did not appear to link the person of interest's girlfriend to the offence and it did not appear that the increased privacy intrusion of accessing LBS for a phone that was not the person of interest's had been adequately considered. The email stated 'we would be very hard pressed trying to justify expenditure of $1000 approx EACH for this incident unless of course further info is received and that urgency for this changes. The best bet would be to ping the girlfriend's phone who is with [redacted] ($6 each and immediate response) and just hope that they love each other lots and do everything together!'

2015–2020

- On 8 January 2015, an investigator asked ACT Policing Intelligence to identify the subscriber details for a service number 'and if it's the cheap carrier we'll get some pings done this week to [redacted]'.

- On 28 January 2015, an investigator sought access to LBS for a mobile phone number. ACT Policing Intelligence accessed the LBS eleven minutes later. The following day an approval (authorisation) form was prepared for the LBS.

- On 17 March 2015, a member of ACT Policing emailed the relevant officer in charge (OIC) advising they had accessed LBS on three occasions the week before and that the paperwork was on the OIC's desk. The email stated 'They were for pings I did on Friday for [redacted] and I completely forgot the paperwork until this evening.'

- On 21 June 2015, a member of ACT Policing raised an issue with the relevant OIC where another member had accessed additional LBS on phone numbers that they had not been approved to search for and that they were 'not aware it was going to be a fishing expedition'.

- On 6 April 2016, a member of ACT Policing advised the OIC that they had reviewed recent tasks and members were not supplying the required justification for the requested access to LBS. The email states 'While I have asked my team to be flexible and reasonable with this if it gets to the point where the same members/Sgts are not providing the appropriate justification after being prompted on several occasions I will ask them to start rejecting tasks.'

- On 10 May 2016, a member of ACT Policing advised the relevant OIC that LBS had been accessed and that they would submit the approval request 'at some point'. The email stated 'I came to see you re a ping for [redacted] from [redacted] but you were in a meeting. I asked [redacted] to do it as only couple dollars, nil results anyway but you will get the approval request come through at some point. Let me know if you need more info.'

- On 7 June 2016, a member of ACT Policing sought approval from the relevant OIC to undertake telecommunications checks. Two minutes later, the OIC provided approval for the necessary 'IPND, subscriber checks and pings/triangulations required for the investigation', noting that the matter had been discussed. While an authorised officer has the discretion to approve such a request on the basis of the information put before them, the email response does not provide the required record of the authorised officer's decision making. It also does not make it clear the scope of what was authorised or the matters considered to assess privacy.

- On 19 February 2017, a member of ACT Policing provided records indicating they had accessed LBS on 10 occasions. Shortly thereafter, paperwork for approval was prepared for this access.[12]

- On 3 April 2017, a request for access to LBS was provided to the relevant OIC. The OIC advised the requesting member that before they could finalise approval the member should address why call charge records or reverse call charge records would not be sufficient for the matter and that this was 'usually due to timeliness etc'. A number of minutes later, the request was resent to the OIC, advising that CCR/RCCR would not be effective 'due to the timeliness of the investigation.' This was approved within 2 minutes of the request being sent. On 7 March 2018, a request for access to LBS was sent which provided the 'timeliness' justification to the request made on 3 April 2017 in regard to why CCR/RCCR would not be effective as opposed to accessing LBS.

- On 16 January 2019, a member of ACT Policing emailed a colleague with the subject line 'Who's [sic] number am I pinging again?' and indicated they had already accessed the LBS once advised of the name of the person of interest. This indicated an informal approach to the use of a covert power and potentially access that occurred without a signed authorisation, as the relevant number would be stated on the authorisation before the member accessing the LBS.

- On 9 January 2020, a member of ACT Policing emailed the relevant OIC to advise that they were catching up on 'Telco Ping forms/admin' for a number of occasions when LBS had been accessed and wanted to know the correct authorisation form to

[12] The unsigned approval paperwork covers the same reference number as the LBS that had been accessed and the requested financial component would cover precisely 10 LBS.

use. The email states that 'this is all pre your request to immediately stop forced Pings.'

4.16. Our review also identified emails showing repeated but isolated attempts to improve compliance, including that telecommunications data are not accessed without prior authorisation or appropriate justification. For example:

- On 22 February 2012, a senior officer at ACT Policing advised the ACT Policing Intelligence distribution list that there had been inappropriate use of LBS for surveillance purposes and that '…the use of PINGs to locate a phone is to be undertaken only when absolutely necessary…'

- On 16 April 2012, a member of ACT Policing emailed the ACT Policing Intelligence District distribution list providing outcomes from a team leaders' meeting held the same day. Among other matters, this covered the topic of 'pings' where it was noted that several issues had arisen in relation to the appropriate use of this capability. It highlighted that pings 'are not to be used just to find someone to talk to them, to get a starting point for ad hoc surveillance or see if they are home. OIC Intel has made mention that he is seeing a number of Ping requests come through with no real reason why…' and 'We all have to remember there is a legal requirements [sic] for these to pass'.

- On 17 April 2012, the relevant Acting OIC emailed the ACT Policing Intelligence distribution list that '...the issue around the practice of 'pinging phones' has come to notice again. To reiterate the practice of 'pinging' a phone number without the consent of a team leader is to stop immediately...'. The email also noted that 'approval needs to be given **prior** to the "ping" being done' and 'we need to ensure we are using this as it was designed to be used and it is not being abused for the sake of expediency.'

- On 5 March 2015, the relevant OIC, noting that LBS had already been accessed on a mobile phone number on two occasions, advised a member of ACT Policing that LBS needed to be approved by the OIC or relevant Superintendent and that no more access would be approved unless appropriately justified.

- On 22 June 2015, the relevant OIC emailed the ACT Policing Intelligence distribution list advising that it had come to their attention again that LBS was being accessed outside of ACT Policing's guidelines, including accessing LBS without approval.

- On 12 October 2015, the relevant OIC emailed the ACT Policing Intelligence distribution list advising that due to changes to legislation, telecommunications data checks could not be conducted without prior authorisation.[13]

- On 21 October 2015, the relevant OIC emailed an ACT Policing distribution list advising of changes resulting from the introduction of the data retention regime and that members must provide a justification on why telecommunications data is required to ensure compliance. This was accompanied by template wording to assist in meeting those requirements.

[13] It has always been a requirement of the TIA Act that a disclosure was preceded by an authorisation.

- On 26 August 2016, the relevant OIC advised a member of ACT Policing that several criteria needed to be addressed for prospective data requests (LBS) and that other avenues should be exhausted before it could be considered.

- On 14 September 2016, the relevant OIC provided a detailed list of matters that the requesting officer would need to address before a 'ping' could be approved.

4.17. Despite having authorised access to telecommunications data and the attempts made to improve compliance, our review identified emails indicating that authorised officers within ACT Policing did not have a clear appreciation of the TIA Act's requirements. For example:

- On 15 June 2016, the relevant OIC sought assistance to obtain the authorised officer's required legislative considerations for approving telecommunications data requests, noting 'I am trying to find what the considerations are for approving PINGS (Prospective data).'

4.18. Our expectation is that authorised officers should be familiar with Chapter 4 of the TIA Act. This extract from the email above indicated that the OIC, in their capacity as an authorised officer who had approved many of ACT Policing's telecommunications data requests, may not have been sufficiently aware of the TIA Act's core requirements.

4.19. Further, in at least one instance, it appears ACT Policing was aware that issues with its processes could be identified through audits, as the email summary below highlights that scrutiny could be applied to timestamps in SEDNode.

- On 8 October 2015, the relevant OIC emailed themselves a to-do list that included a note that they needed to talk to an ACT Policing member about telecommunications data requests not being sent through SEDNode without authorised officer approval due to time stamps that could be scrutinised.

4.20. Due to the clear lack of understanding by requesting and authorising officers of the requirements to access LBS, the limited improvement in compliance when accessing LBS between 2010 and 2020, and the informal approach taken in using these intrusive powers, we make the following recommendation:

Recommendation 5

In consultation with our Office, the Australian Federal Police (AFP) should implement a compliance focussed approach to using the powers under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*.

Such a program should engender transparency, accountability and self-evaluation through regular and rigorous reviews of authorisations for telecommunications data by Covert Analysis and Assurance (CAA), as the AFP's current centralised compliance team, and regular feedback from these reviews to the cohort of officers involved in accessing telecommunications data.

The program should also include removing an Authorised Officer from the s 5AB instrument so they cannot authorise access to telecommunications data if their authorisations are the subject of repeated and serious compliance findings.

Missed opportunities to identify and remedy ACT Policing's alternative process

4.21. We identified several missed opportunities between 2010 and 2018 at which the AFP and ACT Policing could have addressed ACT Policing's independent use of LBS but did not do so.

AFP awareness of ACT Policing's practices

4.22. Our investigation found that a lack of communication and engagement between ACT Policing and the AFP's centralised compliance team contributed to inconsistencies in the processes and practices used by the two areas and subsequent non-compliance with the legislative requirements of the TIA Act. We also found evidence that some of these processes had not developed in isolation but, rather, had continued with the knowledge of both areas.

4.23. While we could not accurately pinpoint when ACT Policing's approach to accessing prospective telecommunications data outside of the AFP's usual process began, we believe it likely started in 2007, when ACT Policing Intelligence members were given access to SEDNode. From that point onwards, it seems ACT Policing independently established its own processes for accessing prospective telecommunications data without involvement from the AFP's centralised compliance team.

4.24. From 2007, ACT Policing included reference to its ability to obtain LBS in numerous training courses. This capability was also listed in internal procedures from 2010 to 2016 as one of the telecommunications data checks that could be undertaken via ACT Policing Intelligence and listed in ACT Policing Intelligence SOPs from 2010 to 2015.

4.25. ACT Policing's process for accessing LBS was also independent of its own Special Projects Registrar (SPR), through which requests to the AFP's central processing areas would usually be routed for quality assurance. Notably, in 2018 a list of requests that the SPR was responsible for did not reference the LBS capability, and 'cheat sheets' circulated by the SPR in 2018 about access to prospective telecommunications data made reference only to access occurring via the AFP's centralised compliance team.

Events in 2010 to 2017

4.26. In the course of our email audit, we obtained various iterations of the AFP's National Guideline on Access to Telecommunications Data, including a 2010 version which was drafted in consultation with ACT Policing Intelligence. The Guidelines referenced the use of LBS and specifically stated that *'TCD (DTST)[14] shall process all requests for prospective telco data, including, but not limited to:*

- *Mobile location – immediate response (via SEDNode)*
- *LBS continuous update (via SEDNode).'*[15]

[14] The predecessor to TID, now known as CAA, the AFP's centralised compliance team.

[15] 'Mobile location—immediate response' is the formal name for one-off LBS available in SEDNode. 'Mobile location—continuous update' is as described, continually updating information on the location of a mobile phone for the specified interval.

4.27. It was not clear why, either during consultations or the eventual implementation, ACT Policing did not identify that its processes were clearly inconsistent with the National Guidelines.

4.28. Based on emails we reviewed during the investigation, we determined the AFP first became aware of ACT Policing's process in late 2010 and with ACT Policing, established a mechanism through which authorisations would be reported to the AFP for inclusion in Ministerial reporting.

- On 3 November 2010, a senior officer in the AFP's centralised compliance team emailed the relevant Acting OIC at ACT Policing advising that the AFP's centralised compliance team had recently been informed ACT Policing was administering its own s 180 prospective authorisations for LBS via SEDNode and that ACT Policing would need to provide its figures for the financial year for reporting to the Minister.

  The senior officer also stated, 'I think it [sic] also be worthwhile having a quick meeting to discuss what could be implemented procedurally to ensure we are covered from now on.'

- On 3 November 2010, the relevant OIC responded advising that there were 479 authorisations[16] and stated 'will give you a call to discuss further but in a nutshell we will take you up on your offer to store the originals'.[17]
- On 4 November 2010, an email was sent to the ACT Policing Intelligence Staff distribution list advising that all completed forms for s 180 LBS authorisations were to be filed for forwarding to the AFP's centralised compliance team, to enable accurate reporting to the Minister in line with legislative requirements.[18]

4.29. Despite these communications, we did not identify evidence that the procedures for ACT Policing's use of LBS and its reporting of authorisations to the AFP were formalised at that time.

4.30. The arrangement of reporting authorisations to the AFP's centralised compliance team appears to have continued over the next two reporting years. For example, on 30 June 2011 and 15 June 2012 a member of the AFP's centralised compliance team emailed an ACT Policing Intelligence member to discuss ACT Policing's s 180 authorisations as they were collating figures for the annual report.

4.31. The reporting of ACT Policing LBS numbers continued until at least mid–2012, at which point it appears staff turnover created a loss of corporate knowledge within the AFP's centralised compliance team.

4.32. It also appears that, until 2018, ACT Policing continued to send hardcopy authorisations to the AFP's centralised compliance team. This is supported by various

---

[16] A later email on 9 November 2010 corrected this to 65 authorisations. It is likely the figure of 479 represented individual instances of LBS being accessed as opposed to authorisations.

[17] The reference to 'originals' refers to the original authorisations. When the issues that are the subject of this investigation came to notice in January 2020, the AFP was able to identify boxes of original authorisations stored at the AFP's centralised compliance team. Many of these were stamped as 'entered' indicating they had been processed internally.

[18] Statutory reporting under the TIA Act had been a responsibility of the AFP's centralised compliance team since well before this time.

internal guidelines at ACT Policing, such as ACT Policing's SOP and other materials which indicated that copies of authorisations for access to LBS should be placed in a tray for forwarding to the AFP's centralised compliance team.

4.33. This suggests that ACT Policing believed it was following a process that was agreed to by the AFP. However, it remains unclear why—if it was not including this data in its reporting—the AFP did not question the purpose of the batches of authorisations it received. ACT Policing did not question why they were receiving requests for their historic telecommunications usage, but not for their prospective telecommunications statistics (including the number of times they authorised LBS).

4.34. In our review of invoices from the vendor of SEDNode we found that, from March 2016, copies of itemised invoices were sent to a member of the AFP's centralised compliance team responsible for statutory compliance and annual reporting. From March 2016 to December 2017, these invoices included itemised results for LBS pings conducted by ACT Policing. The monthly invoices for this period presented another opportunity for those in the AFP's centralised compliance team to identify ACT Policing's access to LBS outside of AFP's normal processes.

4.35. We consider the perception that a process had continued in isolation at ACT Policing, without the AFP's centralised compliance team's knowledge, can likely be attributed to the fact that staff turnover created a loss of corporate knowledge about the process ACT Policing was using to obtain LBS.

Introduction of Data Retention regime in 2015

4.36. The lead-up to the commencement of the data retention amendments (which amended the TIA Act and established the telecommunications data retention scheme) in October 2015 was an important point at which engagement between the AFP and ACT Policing on processes to access telecommunications data would have occurred.

4.37. Despite this engagement presenting an opportunity for the AFP to identify ACT Policing's use of LBS and/or for ACT Policing to determine that its access was occurring outside the approved process, this did not occur.

4.38. For example, we identified that during this time, members of ACT Policing were provided with all-staff emails, an announcement on the AFP's Investigator's Community of Practice portal, new templates in the Investigator's toolkit and training materials, which, while limited in some respects, advised staff that authorisations for prospective telecommunications data were to be processed by the AFP's centralised compliance team.

4.39. On 14 October 2015 ACT Policing flagged that its forms, including the specially developed template it used for LBS, may need to be deleted from the AFP's corporate document repository. However, it appears this did not occur and ACT Policing continued to use unapproved forms to internally process LBS authorisations.

4.40. Prior to implementing the data retention amendments, the AFP brought together a variety of internal stakeholders to form a Data Retention Implementation Working Group (DRIWG). Correspondence about attendance at the working group's meetings indicates the level of engagement between the AFP and ACT Policing may not have been sufficient, or timely.

4.41. Due to the limited engagement, ACT Policing had not adequately positioned itself to navigate the changes. Had ACT Policing been more closely involved in the implementation phase of the data retention amendments, it is possible that ACT Policing's practice of

accessing LBS outside of the AFP's approved practices could have been identified prior to 13 October 2015 and many of the resultant compliance issues minimised.

4.42. Even after the data retention amendments had been implemented, in early 2016 ACT Policing sought clarification from the AFP's centralised compliance team about which template ACT Policing should use for prospective authorisations and provided links to both the current template managed by the AFP's centralised compliance team and ACT Policing's 'old' LBS template.

4.43. At that time the AFP's centralised compliance team advised that the only template that investigators should use was the template within the investigators toolkit (i.e. the AFP's centralised compliance team's managed template). This template stated it was to be sent to the AFP's centralised compliance team once completed, which should have served as a clear indication that any other process was not an approved process. It appears the AFP's centralised compliance team did not question whether the contact indicated ACT Policing was using processes outside the national framework.

4.44. ACT Policing's inaction following the implementation of the data retention scheme, the development of ACT Policing's internal procedures, and the shortfalls in administrative arrangements discussed above all highlight the lack of effective communication and engagement between the AFP and ACT Policing that contributed to the breaches in ACT Policing's access to LBS. As a result, we make the following recommendation:

Recommendation 6

To avoid inconsistent processes developing in future, the Australian Federal Police should establish regular forums for communicating and engaging with ACT Policing to ensure:

- ACT Policing's procedures for accessing telecommunications data are in line with the AFP's established procedures.

- ACT Policing's operational needs are being met by the AFP's centralised compliance team.

- Information about compliance issues is shared in a timely way.

4.45. We identified further emails which show the existence of ACT Policing's alternative process was brought to the attention of staff members within the AFP's centralised compliance team again in 2017 and 2018. For example, on 8 November 2017 the Acting Team Leader for the AFP's centralised compliance team's Interception Management Team emailed the OIC Intelligence at ACT Policing advising that the AFP's centralised compliance team had become aware ACT Policing Intelligence was utilising SEDNode to request prospective telecommunications data, including LBS and they wished to discuss the process for those requests.

4.46. In the course of our investigation we reviewed emails from 2018 which discussed an ACT Policing authorisation issue, where the s 5AB authorisation instrument omitted a key ACT Policing position and meant ACT Policing did not have an appropriately authorised officer to approve disclosure of telecommunications data. These emails show that, at this time, the AFP had also become aware of ACT Policing's use of LBS outside of established practices and specifically identified that multiple members of the AFP and ACT Policing were aware ACT Policing was using LBS. It was unclear whether the Chief Police Officer was also briefed on the LBS issue in addition to the authorisation issue.

4.47. It is also not clear why the AFP did not disclose the breaches to our Office when they were identified in 2018 and why, during our investigation, neither the AFP nor ACT Policing acknowledged they had been aware of ACT Policing's approach to accessing LBS prior to the disclosure in January 2020.

PART 5: ACTION TO REMEDY BREACHES AND FURTHER ACTION REQUIRED

5.1. Moving forward, the AFP's response to these issues needs to be comprehensive and multi-pronged. Action should encompass:

- ongoing education and training to maintain and increase staff awareness of, and compliance with, their legislative obligations under the TIA Act
- a shift in compliance culture with support from the AFP's senior leadership with a view to improving transparency, accountability, responsiveness and self-evaluation
- compliance-focused guidance and procedures that are simple, comprehensive and easily accessible to support staff in confidently navigating and understanding the legislative framework
- consequences for authorised officers who demonstrate continued non-compliance with legislative requirements
- engagement with other agencies and our Office regarding implementing better practice.

5.2. Following the PwC audit report, the AFP removed access to SEDNode for all users outside of the AFP's centralised compliance team. The AFP also centralised all access to telecommunications data under the TIA Act within their centralised compliance team. This meant that ACT Policing, which previously had access to historic telecommunications data under an AFP-approved independent process, must now make all requests for telecommunications data via the centralised compliance team.

5.3. In the course of our investigation, the AFP provided our Office with training materials related to accessing telecommunications data. This included its 'Introduction to Accessing Telecommunications Data (Training Program 2020)' slides, 'requesting access to historical telecommunications information checklist' and approvals flowcharts. Privacy considerations are not referenced in these training and process documents. The AFP subsequently advised that this training is an adjunct to mandatory training packages which contain specific information relating to privacy considerations.

5.4. In accordance with the TIA Act, the privacy intrusion in accessing telecommunications data must be justified based on the seriousness of the matter being investigated and the likely usefulness of the information gained.

5.5. The AFP has committed to undertaking an annual 'control audit' (conducted by its Internal Audit team) to test compliance against the mitigation strategies it has put in place to prevent further non-compliance. While our Office supports an increased focus on compliance at the AFP, we are concerned this process may not be a sufficient control. In particular, the methodology approved by the Assistant Commissioner (Crime Command) considers the requesting officers' privacy considerations and authorising officers' comments and privacy considerations for granting requests as 'Authorisation extras' that are 'preferably included (but not fully enforced)'. However, these considerations are integral to compliance with the TIA Act and the obligation to keep records is explicit, so we suggest that, by not requiring staff to record privacy considerations, the AFP leaves itself open to the risk of continued non-compliance.

5.6. Due to the:

- lack of records to show the required considerations had been made by authorised officers
- previous recommendations we have made to the AFP about authorised officers making and documenting the required considerations
- limited guidance in past and current training materials on making and documenting the required considerations, particularly in regard to privacy, we make the following recommendation:

Recommendation 7

The Australian Federal Police (AFP) implement a consistent mechanism for authorised officers to demonstrate they have made the required considerations to authorise access to telecommunications data under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act), including that the privacy intrusion is justified and proportionate.

The AFP should also ensure training and any other supporting documentation for requesting and authorised officers provides detailed guidance on the considerations authorised officers are required to make and document under the TIA Act, in particular that the privacy intrusion is justified and proportionate.

5.7. Where previously ACT Policing could undertake a single LBS of a service number via SEDNode, as a result of the centralisation of all access to telecommunications data under the TIA Act with the AFP's centralised compliance team, the current process is now to request call-associated data (CAD) through the AFP's interception platform. An authorisation provisioned as CAD through the interception platform would result in more data being obtained, at more regular intervals, than access to LBS via SEDNode.

5.8. As such, we consider that due to its ongoing nature, the use of CAD provisioned via the AFP's centralised compliance team and the AFP's interception platform may result in increased privacy intrusion when contrasted against accessing LBS through SEDNode for one or a number of LBS only. We therefore make an additional recommendation regarding this potential for increased privacy intrusion:

Recommendation 8

The Australian Federal Police (AFP) examine any increased privacy intrusion in the use of call associated data in circumstances where telecommunications data could alternatively have been accessed through an LBS via SEDNode and where it is determined that the privacy intrusion would be reduced by using SEDNode, preference this approach ahead of using call associated data.

APPENDIX A: THE AFP'S RESPONSE TO RECOMMENDATIONS

Recommendation 1
To ascertain whether other areas of the Australian Federal Police (AFP) have accessed LBS, the AFP should obtain and audit all data from SEDNode for all users, to the extent that data is available, to determine the number of requests made for LBS, covering the period from 13 October 2015 to 31 January 2020. The AFP should also continue to monitor the use of SEDNode nationally, to ensure that business areas access appropriate request types in line with their designated roles.
The AFP's Response
The AFP accepts this recommendation and is working with SEDNode, undertaking an audit of all relevant data. Process changes have been implemented to ensure that SEDNode access is appropriately managed.
Recommendation 2
The AFP include any LBS authorisations made outside ACT Policing between 13 October 2015 and 31 January 2020 in records for our Office's next inspection of the AFP's compliance with Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*.
The AFP's Response
The AFP accepts this recommendation, all located outstanding authorisations will be included in the next routine inspection of the AFP's compliance with Chapter 4 of the *Telecommunications (Interception Access) Act 1979*.
Recommendation 3
The Australian Federal Police (AFP) should seek legal advice on any implications arising from accessing prospective telecommunications data that has not been properly authorised. A) Where it has been identified that prospective telecommunications data has been accessed without the proper authorisation, or where the AFP is unable to determine that the authorisation complied with legislative requirements, an assessment should be made by the AFP to determine whether the prospective telecommunications data has been used for any evidential or prosecutorial purposes. B) Where the AFP has determined that unauthorised prospective telecommunications data has been used for evidential or prosecutorial purposes, legal advice should be sought by the AFP to assess any implications of each individual use of the unauthorised prospective telecommunications data. C) The AFP should quarantine all records where a written authorisation was not in place before prospective telecommunications data was accessed until after our Office's 2021–22 inspection of the AFP's compliance with Chapter 4 of the Telecommunications

(Interception and Access) Act 1979, after which time the unauthorised data should be destroyed.
The AFP's Response
The AFP accepts this recommendation and has sought preliminary legal advice to address all points made in this recommendation.
Recommendation 4
The Australian Federal Police should revise its reporting of all authorisations for prospective telecommunications data under s 186 of the *Telecommunications (Interception and Access) Act 1979* to the Minister for Home Affairs between 1 January 2009 and 30 June 2020 to ensure all authorisations for access to prospective telecommunications data have been included and provide addendums to the Minister for Home Affairs, as required.
The AFP's Response
The AFP accepts this recommendation, addendums will be made to revise reporting as required.
Recommendation 5
In consultation with our Office, the Australian Federal Police should implement a compliance focussed approach to using the powers under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*. Such a program should engender transparency, accountability and self-evaluation through regular and rigorous reviews of authorisations for telecommunications data by Covert Analysis and Assurance (CAA), as the AFP's current centralised compliance team, and regular feedback from these reviews to the cohort of officers involved in accessing telecommunications data. The program should also include removing an Authorised Officer from the s 5AB instrument so they cannot authorise access to telecommunications data if their authorisations are the subject of repeated and serious compliance findings.
The AFP's Response
The AFP accepts this recommendation and is currently in the process of initial assessment, determining what this approach and program would involve and how it will be consumed by the broader organisation.
Recommendation 6
To avoid inconsistent processes developing in future, the Australian Federal Police should establish regular forums for communicating and engaging with ACT Policing to ensure: - ACT Policing's procedures for accessing telecommunications data are in line with the AFP's established procedures.

- ACT Policing's operational needs are being met by AFP's centralised compliance team.
- Information about compliance issues is shared in a timely way.

The AFP's Response

The AFP accepts this recommendation. Covert Analysis and Assurance and ACT Policing have already established regular reoccurring forums and have clear communication lines to address issues of compliance, consistency and timeliness.

Recommendation 7

The Australian Federal Police implement a consistent mechanism for authorised officers to demonstrate they have made the required considerations to authorise access to telecommunications data under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act), including that the privacy intrusion is justified and proportionate.

The AFP should also ensure training and any other supporting documentation for requesting and authorised officers provides detailed guidance on the considerations authorised officers are required to make and document under the TIA Act, in particular that the privacy intrusion is justified and proportionate.

The AFP's Response

The AFP accepts this recommendation and will address this through pending changes in the authorisation process.

Recommendation 8

The Australian Federal Police examine any increased privacy intrusion in the use of call associated data in circumstances where telecommunications data could alternatively have been accessed through an LBS via SEDNode and, where it is determined that the privacy intrusion would be reduced by using SEDNode, preference this approach ahead of using call associated data.

The AFP's Response

The AFP accepts this recommendation and will make changes through both process and education.

APPENDIX B: KEY FINDINGS FROM INSPECTIONS

Inspection details	Key issues, recommendations and AFP's remedial action
Inspection conducted in 2015–16 This was the first time agencies were subject to our oversight of telecommunications data powers. The results of these inspections served as a baseline or 'health check' assessment and enabled us to work with each agency to identify their individual strengths and risks of non-compliance with Chapter 4 of the TIA Act.	***ACT Policing instrument of authorisation*** Section 5AB(1A) of the TIA Act states that the Commissioner of Police (of the AFP) may authorise in writing a senior executive employee within the AFP to be an 'authorised officer'. Under the TIA Act, only an authorised officer may authorise the disclosure of telecommunications data. During the health check inspection in November 2015, the AFP disclosed that, due to an administrative oversight, the Commissioner's written authorisation under s 5AB(1A) of the TIA Act did not include any officers within ACT Policing. As a result, an officer of ACT Policing who was not authorised (but understood they were) made 116 authorisations during the period relevant to our inspection. The officer also made a large number of authorisations dating back to March 2015, prior to the commencement of our Office's oversight on 13 October 2015. Upon identifying the error, the AFP updated the Commissioner's written authorisation on 26 October 2015 to appoint the relevant position within ACT Policing as an authorised officer.
Non-routine inspection (conducted on 5 May 2017) In April 2017, the AFP disclosed to our Office a breach of the TIA Act, whereby it had accessed telecommunications data pertaining to a journalist without a journalist information warrant being issued. Due to the seriousness of the issue, in May 2017, our Office conducted a 'non-routine' inspection into the breach (under the TIA Act, the Ombudsman may decide to conduct an additional inspection at any time in	***Accessing a journalist's telecommunications data without a warrant*** Section 180H of the TIA Act states that an authorised officer must not make an authorisation that would authorise the disclosure of information or documents of a particular person if the authorised officer knows or reasonably believes that particular person to be a journalist or an employer of a journalist—and a purpose of 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. The AFP's Professional Standards Command (PRS) disclosed it had accessed the telecommunications data of a journalist for the purpose of identifying the journalist's source without a warrant. Our inspection identified the following factors that contributed to the disclosed breach:

response to issues of serious concern).	• insufficient awareness surrounding journalist information warrant requirements within the area of the AFP where the breach occurred • several officers did not appear to fully appreciate their responsibilities when exercising telecommunications data powers • the AFP's heavy reliance on manual checks and corporate knowledge for preventing applications for access to telecommunications data that do not meet relevant thresholds from being progressed • guidance documents were not effective as a control to prevent this breach. As a result of our inspection, we made the following 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*.' We also suggested 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. We suggested this supplementary training package should cover roles and responsibilities with regards to telecommunications data, highlighting the higher thresholds for instances involving applications regarding journalists. In response to our recommendation, the AFP advised it was finalising an online mandatory training package that all AFP authorised officers would need to complete annually to maintain their authorised officer status. In response to the breach the AFP amended the level of seniority for authorised officers able to issue authorisations under journalist information warrants, limiting the number of people who may issue an authorisation in those circumstances (the delegation for this was updated on 1 August 2017). The AFP also amended templates, reviewed SOPs and guidance documents, and reminded all staff about the requirement to obtain a journalist information warrant in the relevant circumstances.

Inspection conducted 2016–17	***Follow up of ACT Policing instrument of authorisation issue*** During this inspection, we found the AFP had not taken sufficient action to manage the data it received in response to authorisations made by the ACT Policing officer who was excluded from the instrument of authorisation. The AFP advised in April 2018 that the affected information had not been quarantined and the AFP was seeking legal advice regarding the use of the affected information. ***Other issues*** We also identified procedural issues related to telecommunications data searches that were undertaken outside of the parameters of an authorisation and several instances where the AFP had received telecommunications data that exceeded the parameters of the authorisations.
Follow-up non-routine inspection (conducted September 2018) Our Office conducted a second non-routine inspection at the AFP to review how it had used journalist information warrants since the first non-routine inspection and assess its progress in implementing the recommendation and suggestions in our October 2017 report.	***Progress against previous recommendations and suggestions*** In the instances we inspected, we were satisfied the AFP had appropriately applied the journalist information warrant provisions. We also identified the AFP had made several 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. Our inspection confirmed that all authorised officers had attended the mandatory training and that the AFP had appropriate measures in place to assure itself of this attendance. Although the AFP had made progress, we noted that one suggestion from our October 2017 report was not implemented. We had suggested that PRS staff undergo supplementary induction training relating to telecommunications data, shortly after commencing in the section. Following the inspection in September 2018, the AFP proposed to introduce a mandatory online training program for requesting officers (including those in PRS) in 2019 to foster greater awareness of the journalist information warrant provisions. The AFP also advised that it updated PRS's New Starter Induction Checklist in December 2018. These updates required new staff in PRS to record their acknowledgement of general guidance material related to telecommunications data as well as specific information about the Journalist Information Warrant provisions.

Inspection conducted during 2017–18	***Demonstration of authorised officer considerations*** Under the TIA Act, the role of the authorised officer is a critical control for ensuring telecommunications data powers are being used appropriately. During this inspection we identified, and the AFP disclosed, errors related to authorisations and the role of authorised officers in demonstrating they had regard to the required considerations when authorising access to telecommunications data. We noted the errors related to multiple authorised officers across a number of teams within the AFP. This meant the errors could not be attributed to an individual, team or process but, indicated AFP staff more generally did not have a well-embedded appreciation of the requirements of the TIA Act and the individual responsibilities of authorised officers. We noted this was also a contributing factor to the breach of the journalist information warrant provisions, which we reviewed and reported on in October 2017. Based on these errors, our Office was not satisfied the AFP had demonstrated that authorised officers consistently had regard to the considerations required under the TIA Act and made the following recommendation: 'That the Australian Federal Police implements processes to ensure authorised officers have regard to the required considerations prior to authorising access to telecommunications data under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*.' In response, the AFP advised it released an online mandatory training package for authorised officers in November 2017 and all authorised officers were required to complete the training annually. The AFP also released a supplementary training and reference tool and implemented template changes to assist in demonstrating the regard authorised officers had to the required considerations.
Inspection conducted during 2018–19	***Progress against previous recommendations and suggestions*** At this inspection we concluded that, while the AFP had taken remedial action to address the majority of the issues raised at our previous inspection, it had not made enough progress in addressing the previous recommendation regarding authorised officer considerations.

	For example, we identified several instances where we could not confirm the authorised officer had regard to the required considerations before authorising the disclosure of telecommunications data. Many requesting officers' requests for authorisation did not include detailed background information or referred only to case numbers or operations and as such, we were not able to assess what, if any, additional information the authorised officer may have had regard to when making the authorisation. We concluded the AFP's authorised officers did not have a consistent practice for documenting their considerations when making an authorisation. Due to the lack of information in applications and the limited records made by authorised officers, we were not able to assess what information authorised officers had regard to when making their authorisation and whether they had considered all matters required by the TIA Act. Due to the ongoing nature of the issue, we made the following recommendation: 'The Australian Federal Police implements processes to ensure authorised officers consistently document any information relevant to considering and approving a telecommunications data authorisation under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* to demonstrate that the authorised officer took into account all relevant matters, in line with the record keeping requirements under s 186A(1)(a)(i).'
Inspection conducted during 2019–20	***Progress against previous recommendations and suggestions*** At this inspection we again concluded that, while the AFP had taken remedial action to address the majority of the issues raised at our previous inspection, it had not made enough progress in addressing the previous recommendation regarding authorised officer considerations. During this inspection, we again identified a number of instances where we could not determine if the authorised officer had regard to the required considerations before authorising the disclosure of telecommunications data. At this inspection we noted that, while the AFP has detailed guidance materials that require authorised officers to make and record relevant considerations before they authorise the disclosure of

	telecommunications data under the TIA Act, this guidance was applied inconsistently by authorised officers across the AFP. For prospective telecommunications data authorisations, the template includes the grounds for the request and the privacy considerations but provides limited guidance about what should be addressed in the application. The template also doesn't prompt the authorised officer to record their considerations. Many of the prospective authorisations we assessed included limited information to demonstrate the considerations the authorised officer had made. We identified authorisations that only included incomplete template wording, or limited information supporting the proposed authorisation. These records did not have sufficient information to demonstrate the considerations the authorised officers had made. In response to this finding, the AFP advised that in November 2019, the prospective authorisation forms were amended to include a free text field for "authorising officer comments and privacy considerations for granting request."

APPENDIX C: GLOSSARY

Term (and section of the TIA Act)	Description
Access	A law enforcement agency accesses telecommunications data following disclosure of the data by a carrier.
AAT	Administrative Appeals Tribunal
Administrator of the *Telecommunications (Interception and Access) Act 1979* (TIA Act)	Following the *Administrative Arrangements Order – amendment made 1 February 2020*, the Minister for Home Affairs is responsible for administering the TIA Act.
Administrative errors	This includes errors made within administrative processes such as document preparation, statistical reporting and record-keeping. Administrative errors are often a result of human error and may not impact on the validity of an authorisation. However, some administrative errors result in instances of technical non-compliance. Our Office reports on administrative errors where actual non-compliance has occurred, or there is a risk of non-compliance where the error is not rectified.
Annual reporting s 186	Agencies are required to report the number of authorisations they have made within a financial year, to the Minister, within 3 months from 30 June. Also referred to as Ministerial reporting.
Authorisation for access to telecommunications data ss 178-180B and s 183	An authorisation for access to telecommunications data under Chapter 4 of the TIA Act permits carriers to disclose information or documents to enforcement agencies. *Historic authorisation*s Agencies may authorise the disclosure of specified information or documents that came into existence before the carrier receives notification of the authorisation. Historic authorisations can be made where the authorised officer is satisfied that the disclosure is reasonably necessary for: • enforcing the criminal law (s 178). • the purpose of finding a person who the Australian Federal Police or a Police Force of a state has been notified is missing (s 178A). Section 178A authorisations can only be made by the AFP or a Police Force of a state. • enforcing a law imposing a pecuniary penalty or protecting the public revenue (s 179). *Prospective authorisations* Under s 180 of the TIA Act, criminal law-enforcement agencies may authorise the disclosure of specified information or documents that come into existence while an authorisation is in force, if satisfied that the disclosure is reasonably necessary for investigating a serious offence (as defined in s 5D of the TIA Act) or an Australian offence that is punishable by imprisonment for at least three years.

	Prospective authorisations come into force at the time the carrier receives notification of the authorisation and, unless revoked earlier, cease to be in force at the time specified in the authorisation, which must be no later than 45 days from the day the authorisation is made. *Note that different requirements apply for the period in which authorisations made under journalist information warrants are in force.* *Foreign authorisations* Under s 180A of the TIA Act, the AFP can authorise disclosure of specified information or documents that come into existence before the carrier receives notification of the authorisation. Matters about which the AFP must be satisfied in making the authorisation are set out in s 180A(3) of the TIA Act. Under s 180B of the Act, the AFP can authorise disclosure of specified information or documents that come into existence while an authorisation is in force. Matters about which the AFP must be satisfied in making the authorisation are set out in s 180B(3) of the Act. Authorisations under s 180B of the TIA Act come into force at the time the carrier receives notification of the authorisation and, unless revoked earlier, cease to be in force at the time specified in the authorisation, which must be no later than 21 days from the day the authorisation is made, unless this period is extended. *Form of authorisations* An authorisation for disclosing telecommunications data must be in written or electronic form and meet the requirements outlined in the s 183 Determination.
Authorised officer s 5	An authorised officer is an officer with the power to make, or revoke, authorisations for disclosing telecommunications data. The Commissioner of Police may authorise, in writing, a senior executive AFP employee who is a member of the AFP to be an authorised officer (s 5AB(1A)). Our Office considers that authorised officers are a critical control for ensuring telecommunication data powers are used appropriately.
Better practice suggestion	In inspection reports, better practice suggestions are suggestions that our Office considers would further improve agencies' practices and procedures if implemented, and reduce risk of non-compliance with the Act. It is important to note that better practice suggestions do not reflect the existence of non-compliance or a shortcoming on the agency's part.
Carrier	A service provider who supplies certain carriage services over a telecommunications network. Carriers in Australia include (but are not limited to): • Telstra Corporation Ltd • Singtel Optus Pty Ltd • Vodafone Hutchison Australia Pty Ltd.

Chief officer s 5	The head of an agency. For example, the Commissioner of Police is the chief officer of the Australian Federal Police.
Communications Access Coordinator Determination (s 183 Determination) s 183(2)	*Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2015 (superseded as at 20 November 2018 by the below)* *Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2018* The above determinations were made under s 183(2) of the TIA Act, which specifies that the Communications Access Co-ordinator may, by legislative instrument, determine requirements of the form of authorisations, notifications and revocations relating to telecommunications data.
Criminal law-enforcement agency s 110A	Section 110A of the TIA Act defines criminal law-enforcement agencies, which includes the AFP.
Disclosure by agencies to our Office	Prior to, or at the commencement of an inspection, agencies may make a disclosure to our Office outlining an instance, or instances, of non-compliance with the TIA Act. Our Office's inspection reports outline the details of disclosed non-compliance and any agency actions to correct or manage the non-compliance. Disclosures may not be reported in inspection reports if they are primarily administrative in nature. We encourage agencies to make disclosures to our Office following self-identified instances of non-compliance.
Disclosure of telecommunications data	A carrier makes a disclosure of telecommunications data (information or documents) to an agency, following notification of an authorisation. For example, an agency notifies a carrier of an authorisation through a secure system. The carrier responds by making a disclosure of telecommunications data to the agency, also within the secure system. The telecommunications data disclosed must fall within the parameters specified in the authorisation.
Exit interview	Following an inspection, an exit interview is held with officers of the agency and inspection officers from our Office. Preliminary inspection findings are presented, and the agency is given the opportunity to comment.
Historic authorisation ss 178, 178A, 179	A historic authorisation enables access to information or documents that came into existence before a carrier receives notification of an authorisation. The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for: • enforcing the criminal law • locating a missing person • enforcing a law imposing a pecuniary penalty or for protecting public revenue.
Journalist information warrant s 180H and s 180Q-W	An enforcement agency must obtain a Journalist Information Warrant (JIW) when it seeks to access the telecommunications data of a journalist (or their employer), if a purpose of making the authorisation would be to identify another person whom the

	authorised officer knows, or is reasonably believed to be, a source of that journalist. To obtain a JIW, an enforcement agency must apply externally to an eligible Judge, Magistrate or Administrative Appeals Tribunal member, who has been appointed by the Attorney-General. The issuing authority must not issue a JIW unless they are satisfied, for example, that the warrant is reasonably necessary for purposes outlined under subsection 180T(2) of the Act, 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. JIWs 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 JIW.
Minister	The Minister for Home Affairs.
Non-compliance	In the context of our Office's oversight mechanism, an agency demonstrates non-compliance when it has not met a requirement or requirements, of the TIA Act.
Notification to carrier s 184	When a telecommunications data authorisation or revocation is made, it is notified to the carrier.
Pre-inspection data	Data provided by agencies to the Commonwealth Ombudsman prior to an inspection that shows how many authorisations were applied for and the associated reference numbers for those authorisations.

Privacy considerations
s 180F
	Section 180F of the Act outlines the privacy considerations that must be made by an authorised officer before making a telecommunications data authorisation.
	
	The authorised officer considering making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use of information or documents is justifiable and proportionate, having regard to the following matters:
	• the gravity of any conduct in relation to which the authorisation is sought, including:
	  • the seriousness of any offence in relation to which the authorisation is sought
	  • the seriousness of any pecuniary penalty in relation to which the authorisation is sought
	  • the seriousness of any protection of the public revenue in relation to which the authorisation is sought
	  • whether the authorisation is sought for the purposes of finding a missing person.
	• the likely relevance and usefulness of the information or documents
	• the reason why the disclosure or use concerned is proposed to be authorised.

Prospective authorisation s 180	A prospective authorisation enables access to information or documents that come into while an authorisation is in force. A prospective authorisation may also authorise the disclosure of 'historic' data – telecommunications data that came into existence before an authorisation comes into force. Authorised officers must not make a prospective authorisation unless the disclosure is reasonably necessary for investigating a serious offence, or an offence against the law of the Commonwealth, a state or territory that is punishable by imprisonment for at least 3 years. Prospective authorisations come into force at the time the person from whom the disclosure is sought receives notification of the authorisation. The 'person' is often the carrier who holds the telecommunications data. Unless the authorisation is revoked earlier, or is an authorisation made under a journalist information warrant, the authorisation ceases to be in force at the time specified in the authorisation. This time must be no more than 45 days after the authorisation is made. For example, a prospective authorisation is made on 1 March 2019 for all telecommunications data relating to a specified telecommunications number. The authorisation is in force until 31 March 2019. The authorisation is notified to Telstra at 12pm on 2 March 2019. Telstra is then required to disclose all telecommunications data relating to the number from 12pm 2 March 2019 to 11:59pm 31 March 2019.
Quarantine	In the context of managing telecommunications data, the term 'quarantine' means to restrict the use of information through removing access to that information by physical, electronic or other means. For example: if an agency receives information outside the parameters of a telecommunications data authorisation, the agency may quarantine the information by: • storing the information on a separate disc and locking the disc away from investigators • copying the information to a separate password protected file, accessible only to nominated officers • other actions in line with agency policies and procedures.
Recommendation	In an inspection report a recommendation may be made to an agency where significant non-compliance and/or deficiencies in agency processes are identified on inspection.
Remedial action	Remedial action is steps taken by an agency to address a finding that our Office has made as a result of an inspection.
Requesting officer	Within an agency, a requesting officer is an officer who makes a request for a telecommunications data authorisation. The requesting officer is typically an agency investigator, or other person with intimate knowledge of the investigation. The request is forwarded to an authorised officer for their consideration. The request typically contains: • details of the investigation involving the serious offence, or missing person, or pecuniary penalty

	• relevant person(s) and service(s) • the relevance or usefulness of the telecommunications data sought • privacy considerations.
Revocation 180(7)	Under s 180(7) of the TIA Act, an authorised officer of a criminal law-enforcement agency must revoke an authorisation if they are satisfied that the disclosure is no longer required, or if the authorisation is made under a JIW, the warrant is revoked.
Serious contravention s 5E	Section 5E(1) of the Act defines a serious contravention as a contravention of a law of the Commonwealth, a state or a territory that: (a) is a serious offence; or (b) is an offence punishable: (i) by imprisonment for a period, or a maximum period, of at least 3 years; or (ii) if the offence is committed by an individual—by a fine, or a maximum fine, of at least 180 penalty units; or (iii) if the offence cannot be committed by an individual—by a fine, or a maximum fine, of at least 900 penalty units; or (c) could, if established, render the person committing the contravention liable: (i) if the contravention were committed by an individual—to pay a pecuniary penalty of 180 penalty units or more, or to pay an amount that is the monetary equivalent of 180 penalty units or more; or (ii) if the contravention cannot be committed by an individual—to pay a pecuniary penalty of 900 penalty units or more, or to pay an amount that is the monetary equivalent of 900 penalty units or more.
Serious offence s 5D	Section 5D of the Act lists those offences classed as a 'serious offence' for the purposes of the Act. Serious offences include, but are not limited to: murder, kidnapping, theft, drug trafficking and other drug offences, cybercrime, dealing in proceeds of crime, bribery or corruption offences, insider trading.
Standard Operating Procedures	Standard operating procedures, or SOPs, are an agency's written documents that provide guidance on how to undertake actions.
Subscriber	A person who rents or uses a telecommunications service.
Suggestion	In an inspection report, a suggestion may be made to an agency to improve the agency's compliance with the Act. A suggestion is the first line approach to any non-compliance where the agency needs to undertake additional things to stop it reoccurring. These often suggest improvements to processes or suggest that an agency cease a particular process.
Telecommunications data	Telecommunications data is information about an electronic communication, which does not include the contents or substance of that communication. Telecommunications data includes, but is not limited to: • subscriber information • the date, time and duration of a communication • the phone number or email address of the sender and recipient of a communication

	• Internet Protocol (IP) address used by the person of interest while accessing/using internet-based services • the start and finish time of each IP session • the amount of data up/downloaded • the location of a mobile device from which a communication was made.
Template	A model used for arranging information in a document. A template often forms the 'skeleton' of a document, where users can input information into defined fields. Information can also be pre-filled into a template.
Toolkit	An electronic hub available on the AFP intranet providing guidance on various investigative practices, including access to telecommunications data.
Typographical errors	A mistake in typed or printed text, often caused by striking the improper key on a keyboard.
Use and disclosure s 186A(1)(g)	Agencies must keep all documents and other materials which indicate the disclosure and use of information obtained under Chapter 4 of the TIA Act.
Verbal authorisation	We refer to verbal authorisations having been made where a disclosure of telecommunications data is made to an agency without a written or electronic authorisation signed by an authorised officer in place. This practice is **not** permitted under the TIA Act. There are no provisions under the TIA Act to make verbal authorisations, even in urgent or out of hours situations. All authorisations for telecommunications data must be in writing or electronic form and signed by an authorised officer.

APPENDIX D: COMMONWEALTH OMBUDSMAN TELECOMMUNICATIONS DATA INSPECTION CRITERIA

Objective: To determine the extent of compliance with Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) by the agency.

1. Is the agency only dealing with lawfully obtained telecommunications data?

1.1 Were authorisations for telecommunications data properly applied for, given and revoked?

Process checks

P.1.1.1: Does the agency have effective procedures in place to ensure that authorisations are properly applied for, and are they sufficient?

P.1.1.2: Does the agency have effective controls, guidance and training in place for requesting and processing officers to ensure they have sufficient understanding of compliance obligations?

P.1.1.3: Does the agency have effective controls, guidance and training in place for authorised officers to ensure that authorisations are properly given?

P.1.1.4: Does the agency have effective procedures in place to identify when prospective authorisations are no longer required and should be revoked, and to notify carriers of any revocations?

Records checks in the following areas

R.1.1.1: Whether authorisations were in written or electronic form as required by the Act

R.1.1.2: Whether authorisations, notifications and revocations complied with the form and content requirements as determined by the Communications Access Coordinator (s 183(1)(f)) of the Act

R.1.1.3: Whether there is evidence of sufficient information before an authorised officer, prior to them making an authorisation, to enable them to properly consider the matters listed in s 180F of the Act

R.1.1.4: Whether authorisations were only made for information permitted by the Act, with consideration to s 172 of the Act

R.1.1.5: Whether authorised officers have demonstrated that they have considered matters listed under s 180F of the Act, and are satisfied, on reasonable grounds, that the privacy interference is justified and proportionate

R.1.1.6: Whether authorisations were made by officers authorised under s 5AB(1A) of the Act

R.1.1.7: Whether authorisations were made in relation to specified information or documents (ss 178 to 180 of the Act)

R.1.1.8: Whether prospective authorisations are in force only for a period permitted by s 180(6) of the Act

R.1.1.9: Whether prospective authorisations were revoked in relevant circumstances (s 180(7) of the Act)

1.2 Did the agency identify any telecommunications data that was not within the parameters of the authorisation?

Process checks

P.1.2.1: Does the agency have effective and consistent procedures in place to screen and quarantine telecommunications data it obtains?

Records checks in the following areas

R.1.2.1: Whether telecommunications data obtained by the agency was within the parameters of the authorisation

R.1.2.2: Whether the agency identified any telecommunications data (including content) that did not appear to have been lawfully disclosed, and quarantined the data from use (and if appropriate, sought clarification from the carrier)

1.3 Were foreign authorisations properly applied for, given, extended and revoked? (AFP)

Process checks

P.1.3.1: Does the AFP have effective procedures in place to ensure that foreign authorisations are properly applied for, given, extended and revoked, and are they sufficient?

P.1.3.2: Did the AFP ensure that foreign authorisations were only made in relation to permitted information that was not content?

Records checks in the following areas

R.1.3.1: Whether authorisations for telecommunications data on behalf of a foreign law enforcement agency were properly given and disclosed (ss 180A to 180E of the Act)

R.1.3.2: Whether the Attorney-General made an authorisation before a prospective authorisation was made under s 180B of the Act

R.1.3.3: Whether foreign prospective authorisations were properly revoked in accordance with s 180B(4) of the Act

R.1.3.4: Whether extensions of foreign prospective authorisations were properly made in accordance with ss 180B(6) and (7) of the Act

2. Has the agency properly managed telecommunications data?

Process checks

P.2.1.1: Does the agency have secure storage facilities for telecommunications data and associated information?

P.2.1.2: Does the agency have procedures in place to limit access to telecommunications data that it has obtained?

P.2.1.3: Does the agency have processes in place to account for the use and disclosure (and secondary use and disclosure) of telecommunications data?

Records checks in the following areas

R.2.1.1: Whether the use and disclosure (and secondary use and disclosure) of telecommunications data can be accounted for in accordance with s 186A(1)(g) of the Act

3. Has the agency complied with journalist information warrant provisions?

3.1 Does the agency have effective procedures and controls to ensure that it is able to identify the circumstances in which a journalist information warrant is required?

Process checks

P.3.1.1: Does the agency have effective procedures and controls in place to identify the circumstances in which a journalist information warrant may be required?

Records checks in the following areas

R.3.1.1: Whether officers of the agency actively turned their minds to whether a request related to a journalist

R.3.1.2: Whether officers of the agency kept sufficient records around a determination as to whether a request related to a journalist

3.2 Did the agency properly apply for journalist information warrants?

Process checks

R.3.2.1: Does the agency have effective procedures and controls in place to ensure that a journalist information warrant is sought in every instance where one is required (s 180H) of the Act?

R.3.2.2: Does the agency have effective procedures in place to ensure that journalist information warrants are properly applied for and issued in the prescribed form?

Records checks in the following areas

R.3.2.1: Whether the application was made to a Part 4-1 issuing authority (s 180Q(1) of the Act)

R.3.2.2: Whether the application related to a particular person (s 180Q(1) of the Act)

R.3.2.3: Whether the application was made by a person listed under s 180Q(2) of the Act

R.3.2.4: Whether the warrant was issued for a permitted purpose by s 180T(2) of the Act

R.3.2.5: Whether the warrant was in the prescribed form and signed by the issuing authority (s 180U(1) of the Act)

3.3 Did the agency notify the Ombudsman of any journalist information warrants?

Records checks in the following areas

R.3.3.1: Whether the Ombudsman was given a copy of each warrant issued to the agency as soon as practicable (s 185D(5) of the Act)

R.3.3.2: Whether the Ombudsman was given a copy of each authorisation given under the authority of a journalist information warrant, as soon as practicable after the expiry of that warrant (s 185D(6) of the Act)

3.4 Did the agency revoke journalist information warrants when required?

Process checks

P.3.4.1: Does the agency have effective procedures in place to continuously review the need for a journalist information warrant?

Records checks in the following areas

P.3.4.1: Whether the warrant was revoked in the relevant circumstances (s 180W of the Act)

P.3.4.2: Whether the revocation was in writing and signed by the chief officer or their delegate (s 180W of the Act)

4. Has the agency satisfied certain record-keeping and reporting obligations?

Process checks

P.4.1: Does the agency have processes in place which enable it to accurately report to the Minister on the number of authorisations made and journalist information warrants issued, as well as all other matters listed under s 186 of the Act?

P.4.2: Does the agency have effective record-keeping practices in place?

P.4.3: Does the agency have effective record-keeping practices that sufficiently demonstrate compliance, including:

P.4.3.1: Records demonstrating an authorised officer's considerations of the matters listed in s 180F of the Act

P.4.3.2: Records to demonstrate compliant use and disclosure (and secondary use and disclosure)

Records checks in the following areas

R.4.1: Whether the agency sent an annual report to the Minister on time, in accordance with s 186 of the Act and whether the report accurately reflected the agency's use of the Chapter 4 powers

R.4.2: Whether the agency has kept records in accordance with s 186A of the Act

R.4.3: Whether the agency retains all other relevant records to enable our Office to determine compliance, this may include training and guidance documents that are provided to requesting and authorised officers, records of data received or quarantined and file notes addressing discrepancies.

5. Does the agency have a culture of compliance?

Process checks

P.5.1: Is there a culture of compliance?

P.5.2: Does the agency undertake regular training for officers exercising Chapter 4 powers?

P.5.3 Does the agency provide support and appropriate guidance material for officers exercising Chapter 4 powers?

P.5.4: Was the agency proactive in identifying compliance issues?

P.5.5: Did the agency disclose compliance issues to the Commonwealth Ombudsman's office?

P.5.6: Were issues identified at previous inspections addressed?

P.5.7: Has the agency engaged with the Commonwealth Ombudsman's office, as necessary?

P.5.8: Does the agency have processes to ensure compliance, including:

- P.5.8.1: Quality control processes are supported by policy and practical guidance documents?
- P.5.8.2: Effective procedures to measure compliance and identify and action issues as they arise?
- P.5.8.3: Processes and training to identify and track issues that occur?
- P.5.8.4: Protocols for advising relevant officers of issues that arise?