COMMONWEALTH OMBUDSMAN

Commonwealth Ombudsman's annual report

Monitoring agency access to stored communications and telecommunications data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979*

For the period 1 July 2018 to 30 June 2019

Report by the Commonwealth Ombudsman
under s 186J of the *Telecommunications (Interception and Access) Act 1979*

COMMONWEALTH OMBUDSMAN

Commonwealth Ombudsman's annual report

Monitoring agency access to stored communications and telecommunications data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979*

For the period 1 July 2018 to 30 June 2019

Report by the Commonwealth Ombudsman
under s 186J of the *Telecommunications (Interception and Access) Act 1979*

ISSN 2207-4678 (Print)
ISSN 2207-4686 (Online)

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

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

Contents

Executive Summary

This report presents the results of inspections the Office of the Commonwealth Ombudsman (the Office) conducted under s 186B of the *Telecommunications (Interception and Access) Act 1979* (the Act) between 1 July 2018 and 30 June 2019. These inspections assessed agencies' records relating to agencies' use of stored communications and telecommunications data for the period from 1 July 2017 to 30 June 2018.[1]

The Office's role is to provide independent oversight of agencies' use of these covert and intrusive powers, which we achieve by conducting inspections of agencies' records, policies and processes to assess whether their use of the powers complies with the Act. We enhance transparency and public accountability by reporting our findings in this annual report, which the Minister for Home Affairs is required to table in the Parliament.

In 2018–19, we conducted 10 inspections of agencies' use of stored communications powers under Chapter 3 of the Act and 10 inspections of agencies' use of telecommunications data powers under Chapter 4 of the Act. We made 13 recommendations to four agencies. We also made suggestions, including some better practice suggestions, to the agencies inspected.

While we continue to see improvement in most agencies' processes to manage the use of these powers and achieve compliance with the Act, we also identified areas at some agencies where further work is needed to adequately satisfy the Act's requirements. In addition, several issues that we identified during our 2017–18 inspections, were identified again in 2018–19 inspections. While some of these were due to the retrospective nature of our inspections, in some instances we found that agencies had not taken adequate remedial action to address our previous findings.

In our view, this speaks to a critical need for greater overall awareness within some agencies of the Act's requirements and the need for stronger compliance controls.

In saying this, we also acknowledge that a number of our findings were proactively identified and disclosed by agencies. At many agencies, we saw a high level of responsiveness to our inspection findings.

---

[1] Certain aspects of our assessment require us to assess records outside this period in order to capture agency processes as they are being applied.

Part A – Introduction

Under the *Telecommunications (Interception and Access) Act 1979* (the Act) the Office of the Commonwealth Ombudsman (our Office) has an overarching role in assessing agencies' compliance with Chapter 3 (preserving and accessing stored communications) and Chapter 4 (accessing telecommunications data) of the Act.

Stored communications are communications that have already occurred and are stored on a carrier's systems—they contain the content of the communication. An agency must apply to an external issuing authority (such as a judge or eligible Administrative Appeals Tribunal member) for a warrant to access stored communications. Before a warrant is issued, an agency may authorise the 'preservation' of a stored communication to ensure it is retained by the carrier until such time as the communication can be accessed under a warrant.

Telecommunications data is information about a communication, but does not include the content or substance of that communication. Agencies may internally authorise access to this information, subject to a number of conditions and requirements. However, if an agency wishes to access telecommunications data that will identify a journalist's information source, the agency must apply to an external issuing authority for a warrant, before it can make such an authorisation.

Access to stored communications and telecommunications data intrudes on an individual's right to privacy but occurs covertly, so they will not know it has occurred and will not have access to complaint or other review mechanisms that would ordinarily be available if an individual considers action has been taken unreasonably. This makes independent oversight of these powers essential, particularly for telecommunications data powers because the decision to authorise the intrusion into a person's privacy is generally made by the agency rather than an external issuing authority.

Our Office inspects agencies' records to assess the extent of compliance with the Act when agencies use these powers. The Act imposes requirements that must be satisfied by agencies, such as the requirement to weigh the value of the information to be obtained against the reasonableness and proportionality of the privacy intrusion. If agencies cannot demonstrate that they are acting consistently with their legislative obligations, we cannot assure Parliament and the public that these intrusive and covert powers are being used appropriately.

An inspection may identify a range of issues, from minor administrative errors through to serious non-compliance and systemic issues. If an issue is sufficiently serious and/or has been previously identified and not resolved, the Ombudsman may make formal recommendations for remedial action. However, where an issue is less serious, in the first instance we will make suggestions for improvement, to encourage agencies to take responsibility for identifying and implementing practical solutions.

We may also make 'better practice suggestions' where we consider an agency's existing practice may expose it to a risk of non-compliance.

The Ombudsman is required to report the results of these inspections to the Minister for Home Affairs (the Minister), who must table the report in the Parliament.

This report is divided into five parts:

- **Part A** introduces our oversight of agencies' use of powers under Chapters 3 and 4 of the Act, and the approach we took to this role in the 2018–19 inspection period.
- **Part B** highlights the importance of compliance culture.
- **Parts C and D** set out the results of our stored communications and telecommunications data inspections, respectively.
- **Part E** provides a glossary of key terms used throughout the report.

Agencies we oversee

Currently, 20 agencies have access to stored communications and telecommunications data under the Act (see below list). The Minister may declare additional agencies in prescribed circumstances, but did not make any such declarations in 2017–18.[2] We do not oversee telecommunication service carriers.

Agency	Acronym
Australian Criminal Intelligence Commission	ACIC
Australian Competition and Consumer Commission	ACCC
Australian Commission for Law Enforcement Integrity	ACLEI
Australian Federal Police	AFP
Australian Securities and Investments Commission	ASIC
Corruption and Crime Commission Western Australia	CCC (WA)
Crime and Corruption Commission Queensland	CCC (QLD)
Department of Home Affairs	The department
Independent Broad-based Anti-corruption Commission	IBAC
Law Enforcement Conduct Commission	LECC
New South Wales Crime Commission	NSW CC
Independent Commission Against Corruption (New South Wales)	ICAC (NSW)
New South Wales Police Force	NSWPF
Northern Territory Police	NT Police
Queensland Police Service	QPS
Independent Commissioner Against Corruption (South Australia)	ICAC (SA)
South Australia Police	SA Police
Tasmania Police	Tasmania Police
Victoria Police	Victoria Police
Western Australia Police	WA Police

[2] Our inspections in 2018–19 considered use of the powers during 2017–18.

Reduced inspection load

In 2018–19, our Office conducted 10 inspections of agencies' use of stored communications and powers, and 10 inspections of agencies' use of telecommunications data powers. The results of these inspections are set out in **Parts C and D**.

As the Act does not specify the frequency with which inspections must be conducted under Chapters 3 or 4, the Office took a risk-based approach in 2018–19, aimed at balancing its workload for the year. Specifically, during this period the Office did not inspect those agencies with strong mechanisms in place to achieve compliance, or very low use of the powers.

For agencies that were not inspected in 2018–19 we notified them that their records for 2017–18 would be assessed in the subsequent inspection period (2019–20). This ensured our broader oversight of any agencies' use of the powers was not reduced. We will report on the results of these inspections in our 2019–20 annual report.

To ensure engagement with all agencies, we held forums (discussed under the '**Stakeholder engagement'** section below), which brought together different agencies to discuss common issues affecting compliance across the Office's areas of oversight.

How we oversee agencies

We apply a set of inspection methodologies consistently across all agencies. These methodologies are based on the legislative requirements of the Act and better practice standards, and are regularly updated in response to legislative amendments and changes to agency processes. We focus our inspections on areas of high risk, taking into account the potential impact of non-compliance.

We assess compliance based on a sample of records, discussions with relevant agency teams, observations of agencies' processes and agencies' remedial action in response to issues identified. To maintain the integrity of active investigations, we do not inspect records relating to warrants and authorisations that are still in force.

Prior to each inspection we provide our inspection criteria to agencies. This helps agency staff to identify the most accurate sources of information to assist our inspection.

The criteria for our inspections of access to stored communications and telecommunications data are provided at Appendix A and Appendix B, respectively.

We encourage agencies to disclose any non-compliance, including any remedial action they have already taken. Our Office also provides assistance to agencies to achieve compliance by assessing policies and procedures, communicating better practices, facilitating communication across agencies and engaging with agencies outside of inspections.

How we report
To ensure procedural fairness, following each inspection we provide the agency with our preliminary inspection findings verbally at an exit interview and invite its staff to provide any initial comments.

We then provide the agency with a written report containing the results of our inspection and our assessment of their legislative compliance. This can be provided in either a streamlined or formal report format.

We prepare streamlined reports when our inspection findings are not indicative of significant or systemic issues. The instances of non-compliance reported in streamlined reports are typically straightforward and non-contentious. A streamlined report may make suggestions and better practice suggestions to the agency to assist it in achieving compliance with the legislation. We provide these reports directly to the relevant business area of the agency.

We prepare formal reports when our inspection identifies significant or systemic issues or where we consider a formal recommendation is warranted to address legislative non-compliance. Formal reports are generally signed by the Ombudsman and sent directly to the agency's chief officer for action and response. These inspection reports and any subsequent comments on the reports from agencies, contribute to this annual report to the Minister.

Stakeholder engagement
During 2018–19, we provided advice to agencies about compliance issues and better practice in exercising the powers under Chapters 3 and 4 of the Act. This included formal meetings with agencies, as well as ad hoc discussions where agencies contacted us to seek information or advice. This engagement outside of inspections assists our Office to obtain a greater understanding of the issues faced by agencies when applying these powers.

In June and July 2019, we hosted three forums for representatives of the agencies we oversee. The forums, held in Brisbane, Canberra and Melbourne, focused on compliance when using covert and intrusive powers, including under Chapters 3 and 4 of the Act. These events were an opportunity for attendees to discuss better practice and compliance issues. It also provided agencies not scheduled for an inspection during 2018–19 with the opportunity to engage face-to-face with our Office.

Part B – Compliance culture

During our inspection of an agency's use of powers under Chapters 3 and 4 of the Act, we assess its compliance against our inspection criteria. We look at whether the agency:

- was proactive in identifying compliance issues, including disclosing issues
- adequately addressed issues identified at previous inspections
- engaged openly with our Office
- was cooperative and frank.

These factors contribute to our assessment of whether an agency has a culture of compliance.

A strong compliance culture is fundamental to an agency's capacity to comply with the Act. We consider that a strong compliance culture promotes 'compliance self-sufficiency', where agencies can confidently navigate the legislative framework and establish necessary processes to achieve compliance.

Agencies with a strong compliance culture provide effective training and support to staff exercising powers. They have effective induction, training and procedural materials that support staff in understanding their obligations and maintaining awareness of changes to legislation, policy and process. In turn, staff understand why demonstrating compliance is important and, barring human error, generally act consistently with their legislative obligations.

Another indicator of a strong compliance culture is robust internal quality assurance processes which enable agencies to proactively identify risks or issues that may lead to non-compliance with legislative requirements and take appropriate remedial and/or preventative action.

In conducting our inspections, we assess a sample of the agencies' records for the relevant period. While this provides a good level of confidence that we will identify any systemic or significant issues, agencies should not rely on our Office to identify instances of non-compliance or provide solutions for issues identified. It is important that agencies proactively and contemporaneously assess their own records and take appropriate remedial action. This is particularly important given that our inspections are conducted retrospectively and a significant period of time (in some cases over 12 months) may pass, with the agency continuing to make the same errors, before we identify the issue at our inspection.

Agencies with a strong compliance culture also generally demonstrate transparency in disclosing issues to the Office and respond positively to our feedback, recognising it as an opportunity for improvement.

As a result of a strong compliance culture, agencies are also better able to adapt their training and internal guidance in response to changes in legislation, policy and procedure, and are more likely to be given access to new or expanded powers because they have a track record of understanding and applying compliance principles.

Agencies with a strong compliance culture are also likely to be subject to fewer serious adverse findings by our Office and other oversight bodies. In making a recommendation or suggestion as a result of a compliance finding, we consider agencies' compliance mechanisms and culture, which can be a measure of an agency's ability to make necessary changes. This means that, where an agency has strong mechanisms to achieve and support compliance with the Act, we may elect to make simpler findings that focus more on the nature of the non-compliance rather than the precise processes that caused it. We then leave it to the agency to consider how best to implement the recommendation or suggestion and demonstrate its effect at future inspections.

A similar finding at an agency with weaker preventative mechanisms and/or a weaker compliance culture may result in an agency not being able to demonstrate that it has sufficient safeguards to reduce the risk of the issue recurring. This, in turn, would likely result in our Office making a targeted recommendation or suggestion that goes to improving specific processes or mechanisms.

The two case studies below illustrate this approach and the impact an agency's compliance culture can have on its ability to implement improved compliance mechanisms. **Case Study 1** shows the broader effects that the lack of a compliance culture has on an agency's ability to identify and reflect on compliance issues. **Case Study 2** illustrates that responsiveness and proactive engagement by an agency demonstrates a mature compliance culture. This culture enables the agency to effect necessary changes to processes with minimal intervention.

As outlined in **Parts C and D**, we made findings in relation to all agencies inspected during 2018–19. These case studies are included to provide context around certain areas of risk that are relevant to all agencies that exercise powers under Chapters 3 and 4 of the Act, not just the agencies about whom the case study is written.

Case Study 1 – Tasmania Police

During our inspection, we identified that Tasmania Police did not have a well-developed compliance culture. This was indicated by a large number of issues across several of its processes, including limited progress in addressing our previous inspection findings and significant variances in the level of awareness of requirements under the Act. We also identified the need for Tasmania Police to develop processes to assist its staff in meeting their compliance obligations.

While we made specific recommendations and suggestions about the various instances of non-compliance we identified, we considered that the required improvements could not be implemented without fundamental changes to the way Tasmania Police approaches compliance. For that reason, we made two recommendations specifically about Tasmania Police's compliance mechanisms and culture:

- **Recommendation 1—** Tasmania Police implement training and an awareness program to ensure that staff using the powers in Chapters 3 and 4 of the Act have a thorough understanding of the legislative framework and their responsibilities.
- **Recommendation 2—** Tasmania Police develop a compliance program to foster a compliance-focused approach to using the powers under Chapters 3 and 4 of the Act. Such a program requires support from senior leadership and should seek to engender transparency, accountability, responsiveness and self-evaluation.

In response to these recommendations, Tasmania Police advised our Office that it is committed to promoting a strong compliance culture and outlined changes that it expects will increase awareness and compliance among staff. We will monitor the efficacy of these changes at future inspections.

Case Study 2 – Queensland Crime and Corruption Commission

At our inspection of the CCC (Qld), we identified a number of compliance issues which are set out in **Part D** of this report. Addressing these issues required changes to the CCC (Qld)'s telecommunications data authorisation processes and templates.

During and after the inspection, the CCC (Qld) proactively engaged with our Office on the issues we had identified, including proposing revisions to processes and templates. This demonstrated a willingness to own and resolve problems and was indicative of the CCC (Qld)'s commitment to achieving compliance.

Part C – Stored communications

Stored communications and the Commonwealth Ombudsman's oversight function

Under s 186B(1)(b) of the Act, the Ombudsman must inspect records of a criminal law-enforcement agency to determine the extent of compliance by that agency with Chapter 3 when using the stored communications powers. Under s 186J of the Act, the Ombudsman must report to the Minister on the results of inspections conducted under s 186B during each financial year.

Stored communications are communications that have already occurred and are stored in a carrier's systems — they contain the content of the communication. Examples of stored communications include Short Message Service (SMS), Multimedia Messaging Service (MMS), emails and voicemails.

In order to access stored communications, an agency must apply to an external issuing authority (such as a judge or eligible Administrative Appeals Tribunal (AAT) member) for a stored communications warrant. A stored communications warrant authorises an agency to access stored communications held by a carrier that were made or intended to be received by the person in respect of whom the warrant was issued, subject to any conditions or restrictions that are specified on the warrant.

Before a warrant is issued, an agency may authorise the preservation of a stored communication to ensure the carrier retains the communication until it can be accessed under a warrant. There are three types of preservation notices:

- historic domestic preservation notices
- ongoing domestic preservation notices
- foreign preservation notices.[3]

An agency must meet certain conditions under the Act before it can give a preservation notice to a carrier.

We do not assess the merits of a decision by an issuing authority to issue a stored communications warrant. However, we review applications for stored communications warrants, and accompanying affidavits prepared by agencies to assess whether agencies' processes comply with the requirements of Chapter 3 of the Act, and whether the issuing authority was provided with accurate and sufficient information to make the required considerations.

Likewise, we do not review the merits of decisions by agencies to apply for preservation notices but will assess agencies' compliance in giving such notices against the requirements of Chapter 3 of the Act.

[3] Refer to Part E for further explanation of the different types of preservation notices. Note: only the AFP can give a foreign preservation notice.

Other matters that our Office assesses include, but are not limited to the management of accessed stored communications and compliance with record-keeping and reporting obligations. Our inspections criteria for stored communications inspections conducted in 2018–19 are set out in Appendix A.

Summary of stored communications findings

During 2018–19, our Office inspected 10 agencies' access to stored communications under Chapter 3 of the Act, covering records in the period from 1 July 2017 to 30 June 2018.

At many agencies, we saw an increase in the number of compliance-related findings compared to our inspections in 2017–18. However, we note that a number of these findings were proactively identified and disclosed by agencies. We consider the transparency demonstrated by agencies in disclosing issues to our Office and the level of responsiveness to our inspection findings contribute to developing a good compliance culture.

The results of the inspections, while presenting a higher number of findings than in previous years, may, at least in part, be the result of our Office's more expansive assessment of agencies' compliance under Chapter 3 of the Act in 2018–19 when compared to earlier years. In addition to reporting on specific instances of non-compliance by agencies, our inspections in 2018–19 focused heavily on areas of agencies' policies and procedures that may present a risk to compliance with the Act.

Most agencies were receptive to our findings, recommendations and suggestions.

At our 2018–19 inspections we again identified a number of issues that had been highlighted in our 2017–18 inspections. In some instances the retrospective nature of our inspections meant the issues related to records that had already been made at the time of our previous inspection but were not due to be assessed. However, in other instances the issues had simply not been adequately addressed and, as a result, we made further suggestions to guide improvement.

Agencies not inspected in relation to Chapter 3 of the Act during 2018–19
As a result of the risk-based approach applied by our Office in 2018–19, we did not inspect all agencies' compliance with Chapter 3 of the Act (see **Part A**). Agencies we did not inspect were the:

- Australian Commission for Law Enforcement Integrity
- Australian Competition and Consumer Commission
- Australian Securities and Investments Commission
- Corruption and Crime Commission Western Australia
- Independent Broad-based Anti-corruption Commission
- Independent Commission Against Corruption (New South Wales)
- Law Enforcement Conduct Commission
- New South Wales Crime Commission

- Northern Territory Police
- South Australia Police.

Where we did not inspect an agency in 2018–19, relevant records relating to use of the powers in both the period from 1 July 2017 to 30 June 2018 and the period from 1 July 2018 to 30 June 2019 were inspected in 2019–20. The results of those inspections will be included in our 2019–20 annual report.

Compliance issues and risks to compliance

This section outlines instances of non-compliance we identified across multiple agencies during our 2018–19 stored communications inspections, as well as other issues we consider may pose a risk to compliance. We will review agencies' actions in response to these issues, and all other findings from our 2018–19 reports at future inspections.

Training and support provided to officers

At some agencies, we identified a need to improve the training and support they provide to officers when using stored communications powers. We made suggestions and recommendations that agencies bolster awareness of the legislative requirements by delivering education initiatives and developing compliance-focused guidance material. This support is critical in ensuring that agencies can meet their compliance obligations under Chapter 3 of the Act and foster a strong compliance culture.

A lack of awareness or understanding of the importance of legislative requirements may result in stored communications warrants being invalid and stored communications obtained under that warrant being unable to be used. This could, in turn, compromise investigations and/or prosecutions. More generally, a strong compliance culture enhances an agency's ability to identify possible areas of risk of non-compliance and respond appropriately where instances of non-compliance are identified.

Giving preservation notices in a successive manner

During our 2018–19 inspections, we identified that certain agencies had given historic domestic preservation notices in a successive manner on the same basis, or given successive foreign preservation notices in response to a single request by a foreign country. We identified this practice in previous inspection periods, and it remains our position that such practices are not contemplated by the Act.

Where we identified these issues, or agencies disclosed these issues to us, during our 2018–19 inspections, the relevant agency advised us of its action to cease these practices. We will monitor this issue at future inspections.

Historic preservation notices
Criminal law-enforcement agencies may give a preservation notice to a carrier to ensure that the carrier retains communications until they can be accessed under a warrant. A historic domestic preservation notice requires a carrier to preserve the relevant stored communications it holds at any time on the day it receives the notice, while the notice is in force.

In our view, where historic preservation notices are given successively on the same basis, in respect of the same person or telecommunications service and to the same carrier,[4] this simulates the effect of an ongoing domestic preservation notice,[5] a power that is only available to 'interception agencies'. This practice typically results in a carrier preserving stored communications over several days, rather than just those it held on the day the notice was received. In our view this practice may circumvent the intended operation of the Act, noting Parliament legislated two distinct types of domestic preservation notices and drew a distinction between interception and non-interception agencies in the Act.

Foreign preservation notices
If the AFP receives a request from a foreign entity made in accordance with the conditions specified in s 107P of the Act, the AFP must give a foreign preservation notice. A foreign preservation notice requires a carrier to preserve, while the notice is in force, all relevant stored communications that the carrier holds at any time on or before the day it receives the notice.

The foreign entity must then make an access request to the Attorney-General to gain access to these stored communications. If the foreign entity does not make an access request within 180 days from the day the carrier is given the foreign preservation notice, the AFP must revoke the notice. The AFP also must revoke the foreign preservation notice if the Attorney-General refuses the access request or the foreign entity withdraws the preservation request.

There is no provision in the Act for such notices to be renewed, or for a single request from a foreign country to form the basis for an indefinite number of foreign preservation notices. Where successive foreign preservation notices are given in response to a single request from a foreign country, the carrier may preserve further stored communications each time it receives a new notice, potentially resulting in the date range of the stored communications provided exceeding the date range of stored communications the foreign country requested.

[4] For example, giving successive historic domestic preservation notices as a matter of course for the purpose of capturing stored communications across a period of time beyond what the carrier would preserve under one historic domestic preservation notice.
[5] Criminal law-enforcement agencies that are interception agencies may give an ongoing domestic preservation notice requiring a carrier to preserve the relevant stored communications it holds from the day it receives the notice until 29 days later.

Stored communications warrants issued in relation to a victim of a serious contravention

Chapter 3 of the Act contains special provisions in relation to victims of a serious contravention. Where an agency applies for a stored communications warrant to access the stored communications of a victim of a serious contravention, the issuing authority must be satisfied that the victim was unable to consent to their stored communications being accessed, or it was impracticable for the agency to obtain their consent.

During our 2018–19 inspections, we identified that some agencies applied for warrants to access the stored communications of victims in circumstances where there were no records to indicate that the victim was unable to consent or it was impractical to gain their consent.

We identified this issue in previous inspection periods. In 2013 we sought the Attorney-General's department's (AGD) view[6] on the meaning of the terms ‘unable’ and ‘impracticable’ under s 116(1)(da) of the Act. The AGD advised the Office that a person would be deemed ‘unable to consent’ where, for example, they are missing and cannot be located, incapacitated or deceased. Obtaining consent would be deemed ‘impracticable’ where a person’s situation makes contacting them extremely difficult, time-consuming or expensive.

The AGD advised that, if a victim has an opportunity to consent and they do not wish their stored communications to be accessed, then an agency must not use s 116 of the Act to access their stored communications. The AGD also advised that, if a victim declines to give their consent, their reasons for doing so are immaterial.

Where agencies pursue a stored communications warrant in relation to a victim of a serious contravention, they should ensure that the accompanying affidavit accurately reflects whether consent has been sought, and if not, clearly demonstrates how thresholds of ‘unable’ or ‘impracticable’ have been met. Agencies should include any steps taken to obtain a victim’s consent and set out why such action has been unsuccessful. This will enable an issuing authority to make an informed decision about whether to issue a stored communications warrant.

Stored communications warrants issued by an ineligible authority

In order to obtain a stored communications warrant, an agency must apply to an issuing authority. Under s 6DB(1) of the Act, the Attorney-General may appoint a judge, magistrate or certain AAT members as an issuing authority.

During the 2018–19 inspection period, we identified several instances where a person not appointed as an issuing authority under s 6DB(1) of the Act had issued stored communications warrants. As a result, these stored communications warrants were invalid. Where a warrant is invalid, we assess the action the agency has taken to

---

[6] At which time the AGD was the administrator of the Act.

rectify the issue and manage any unlawfully accessed stored communications it has received.

We note that, in all instances, the agencies were unaware that the person was not appointed as an issuing authority at the time the warrants were issued. Agencies often experience difficulty checking the eligibility of issuing authorities as staff generally do not have access to appointment documents and rely on the registrar of the relevant court or tribunal to advise them.

In most instances, we were satisfied the agencies had undertaken remedial action in line with our suggestions. Due to the retrospective nature of our inspections, this issue was also present in records assessed during our 2019–20 inspections.

Destruction of stored communications information

Section 150(1) of the Act sets out the circumstances under which agencies must destroy information or records they obtained by accessing stored communications. Where the chief officer of an agency is satisfied that the information is not required for a permitted purpose, they must cause the information or record to be destroyed forthwith. As the Act does not define 'forthwith', our assessment is guided by what the agency has set as an internal timeframe. Where an agency has not established an internal timeframe, our Office assesses the agency against what we consider to be reasonable based on our understanding of the agency's policies and procedures.

We identified instances of non-compliance with s 150(1) of the Act including:

- destruction of stored communications information that did not take place 'forthwith'
- destruction of stored communications information prior to chief officer approval
- copies of stored communications information that were certified for destruction by the chief officer but had not been destroyed at the time of our inspection.

Following our inspections, agencies generally acted to address these instances of non-compliance. However, given the frequency with which we identified these issues during the 2018–19 inspections and in our 2017–18 inspections, it is clear agencies must act to ensure they have effective destruction processes in place, and provide clear guidance to their staff, so they are well-placed to meet their obligations under the Act.

Authorisations, nominations and appointments

Under the stored communications provisions of the Act, there are several functions and actions that can only be performed under the authority of an authorisation, nomination or appointment.

During our 2018–19 inspections we identified, and agencies disclosed, instances where:

- officers who were not nominated to do so under s 110(3) of the Act applied for stored communications warrants
- officers who were not appointed to do so under s 127(3) of the Act exercised the authority of stored communications warrants
- officers who were not authorised to do so under s 135(2) of the Act received stored communications.

Our assessment of these records indicated that, in these instances, non-compliance was a result of departures from standard procedure, failures to effectively communicate changes in instruments to staff, and/or a lack of consideration of the relevant legislative requirements.

We highlighted similar issues in our 2017–18 annual report. Staff and/or agencies acting without lawful authority is a significant compliance risk that can impact the evidentiary value of the information agencies obtain. It is critical agencies ensure their staff understand the relevant legislative requirements and put strong procedures in place so staff with responsibility for aspects of the stored communications process are appropriately authorised, appointed or delegated to exercise those powers. Agencies must also ensure that any changes in authorisations, nominations and appointments are effectively communicated to staff.

Findings from stored communications inspections conducted in 2018–19

We summarised our key findings below for the 10 agencies we inspected during 2018–19. This does not reflect all issues or findings we raised with agencies.

After receiving our inspection report, agencies often tell us about remedial action they have taken in response to our inspection findings. We review the effectiveness of these actions at our subsequent inspections and include our findings in the appropriate annual report.

1. Australian Criminal Intelligence Commission

We inspected the ACIC from 24 to 28 September 2018. We made **one suggestion** as a result of the inspection and sent the ACIC a report outlining our findings on 12 December 2018.

Table 1 – Stored communications inspection statistics: Australian Criminal Intelligence Commission

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	11	5 (45%)
Ongoing domestic preservation notices	13	11 (85%)
Stored communications warrants	5	4 (80%)

Progress since previous inspection
We did not identify any compliance issues for the ACIC during our 2017–18 inspection.

Significant findings
Condition for giving preservation notice not met
During this inspection, the ACIC disclosed four instances where it gave preservation notices after it had already issued the telecommunication interception warrants it intended to rely on to access the stored communications.

We concluded that the preservation notices were given contrary to the condition under s 107J(1)(d) of the Act, namely that a domestic preservation notice may be given if the agency intends to apply at a later time for a relevant warrant to access the preserved stored communications.

In discussing these records, the ACIC explained that limitations on carrier systems meant that some stored communications were not being captured under the relevant warrant. As such, the ACIC issued preservation notices to ensure the stored communications were not destroyed by the carrier. We noted this explanation and were satisfied this did not represent the ACIC's usual procedures. We suggested the ACIC should document its considerations and decisions in such instances.

Table 2 – Inspection findings: Australian Criminal Intelligence Commission

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Has the agency properly applied the preservation notice provisions?				
Condition for giving preservation notices not met	-	4	1 suggestion	s 107H(2) s 107J(1)(d)

2. Australian Federal Police

We inspected the AFP from 19 to 22 November 2018. We made **two recommendations and 15 suggestions (including four better practice suggestions)** as a result of the inspection. We sent the AFP our final report, incorporating its responses to our draft findings, on 17 December 2019.

Table 3 – Stored communications inspection statistics: Australian Federal Police

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	63	15 (24%)
Ongoing domestic preservation notices	86	17 (20%)
Foreign preservation notices[7]	9	9 (100%)
Stored communications warrants	61	31 (51%)
Destruction of stored communications information	44	44 (100%)

Progress since previous inspection

At our 2017–18 inspection of the AFP, we identified several compliance issues. We identified some of these issues again during the 2018–19 inspection, including instances where the AFP had given successive foreign preservation notices and not destroyed stored communications 'forthwith'.

Significant findings

Giving foreign preservation notices in a successive manner

At this inspection we identified the AFP had continued to give successive foreign preservation notices and made two related recommendations. The AFP acknowledged that it should not give successive foreign preservation notices and advised it would quarantine the stored communications it received and establish procedures and awareness training to mitigate the risk of recurrence.

As discussed in 'Compliance issues and risks to compliance', it is our position that this practice is not contemplated by the Act. There is no provision in the Act for foreign preservation notices to be renewed, or for a single request from a foreign country to form the basis for an indefinite number of foreign preservation notices. Where successive foreign preservation notices are given in response to a single request from a foreign country, the carrier may preserve further stored communications each time it receives a new notice, potentially resulting in the date range of the stored communications provided exceeding the date range of stored communications requested by the foreign country.

[7] Only the AFP may give a foreign preservation notice.

Stored communications warrant applied for in relation to a victim of a serious contravention

We identified one instance where the AFP applied for a warrant to access the stored communications of a victim of a serious contravention. There were no records on file to indicate the victim was unable to consent or that it was impracticable for the AFP to obtain their consent. The AFP advised it quarantined the stored communications.

Warrants issued by an ineligible authority

The AFP was issued with warrants by an AAT member who was not appointed under s 6DB(1) of the Act to issue stored communications warrants. We note the AFP was not the only agency affected by this issue during 2018–19 and it was not aware the AAT member was not appointed at the time the warrants were issued.

When we contacted the AFP, the AAT had already advised it of this issue and the AFP was considering its impact and any necessary remedial actions. The AFP advised us that it quarantined the stored communications it obtained under these warrants.

Stored communications information not destroyed forthwith

At our 2018–19 inspection we identified instances where the AFP had not destroyed stored communications information forthwith, contrary to s 150(1) of the Act. We suggested the AFP implement a process to confirm the location of stored communications information prior to conducting a destruction round, so it can ensure all relevant information is included in the destruction.

The AFP advised it updated its procedures and introduced an additional assurance check to ensure all relevant stored communications information and records are identified and destroyed in line with the legislative requirements.

Directing a carrier to undertake actions that it is not required to do or does not have lawful authority to perform

We identified the AFP had sent correspondence to a carrier which directed it to:

- retain preserved stored communications even though a foreign preservation notice was not in force
- release preserved stored communications in the absence of a stored communications warrant.

There were no records to indicate the carrier had acted on the AFP's directions, but we assessed that the correspondence may have caused the carrier to believe it was legally required to undertake certain actions. It also indicated a lack of understanding by AFP staff of the circumstances in which legally a carrier must act to retain or release stored communications.

We were satisfied that this was an isolated instance and was not consistent with the AFP's usual practice. The AFP acknowledged this finding and confirmed the carrier did not provide any stored communications information as a result of the correspondence.

Table 4 – Inspection findings: Australian Federal Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Stored communications warrant applied for in relation to the victim of a serious contravention	1	-	1 suggestion	S 116(1)(da)
Warrants issued by an ineligible authority	3	3[8]	1 suggestion	s 110(1), s 5(1), s 6DB(1)
Unlawfully accessed stored communications not identified and quarantined	1[9]	-	2 suggestions	s 117
Warrant template not in the prescribed form	General finding	-	1 suggestion	s 118(1)(a), Form 6[10]
Incorrect wording in affidavits	General finding	-	1 better practice suggestion	-
AGD coversheets not completed by carriers	1	-	1 better practice suggestion	-
Directing carrier to undertake action it is not required to take, or does not have lawful authority, to perform	1	-	1 suggestion	s 107N, s 108(2)(a)
Has the agency properly managed accessed stored communications?				
Stored communications information not destroyed forthwith	20[11]	-	1 suggestion	s 150(1)

[8] The AFP advised of a total of six stored communications warrants issued during 2017–18 (including three warrants we identified) and six warrants issued during 2018–19. 2018–19 records were assessed at our next inspection.
[9] This is the number of instances identified, not the number of stored communications unlawfully accessed by the carrier and provided to the AFP.
[10] Form 6 of Schedule 1 of the *Telecommunications (Interception and Access) Regulations 2017 (*the Regulations).
[11] Of 20 instances identified, in three instances stored communications information was located during our inspection despite the records being certified for destruction. This information was subsequently destroyed during our inspection.

Inaccuracies in reporting to the Minister	4	-	2 suggestions	s 150(2)
Has the agency properly applied the preservation notice provisions?				
Giving foreign preservation notices in a successive manner	2[12]	-	2 recommendations	s 107N to s 107S
Preservation notices not revoked	3	5	1 suggestion	s 107L(2)(a)(ii), s 107R(1) and (3)
Has the agency satisfied certain record-keeping obligations?				
Destruction paperwork incomplete	2	-	-	s 151(1)(i)
Keeping records to indicate whether stored communications have been accessed	1	-	1 better practice suggestion	-
Other findings				
Records not included in the AFP's pre-inspection data	9	-	1 suggestion	-
Labelling of discs containing stored communications information	1	-	1 better practice suggestion	-

3. Crime and Corruption Commission (Queensland)

We inspected the CCC (Qld) from 13 to 14 August 2018. We did not make any recommendations or suggestions as a result of the inspection and sent the CCC (Qld) a report outlining our findings on 16 October 2018.

Table 5 – Stored communications inspection statistics: Crime and Corruption Commission (Queensland)

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Ongoing domestic preservation notices	11	11 (100%)
Stored communications warrants	6	5 (83%)

[12] This is the number of instances identified where successive foreign preservation notices were issued in response to a single request from a foreign country, not the number of successive preservation notices given.

Progress since previous inspection
Our 2018–19 inspection of the CCC (Qld) again identified one of the issues we highlighted at our 2017–18 inspection, being that stored communications warrants were not in the prescribed form required by s 118(1)(a) of the Act. This was a minor administrative issue which the CCC (Qld) addressed by updating its stored communications warrant templates.

Significant findings
Stored communications accessed by an unauthorised officer
We identified one instance where a CCC officer, who was not authorised to do so under s 135(2) of the Act, received stored communications. However, we were satisfied that this was an isolated instance. The officer had accessed the stored communications believing they were authorised to do so and the instance did not indicate a broader compliance issue at the CCC (Qld).

Table 6 – Inspection findings: Crime and Corruption Commission (Queensland)

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Warrants not in prescribed form	2	-	-	s 118(1)(a), Form 6
Has the agency properly applied the preservation notice provisions?				
Stored communications accessed by an unauthorised officer	1	-	-	s 135(2)

4. Department of Home Affairs

We inspected the Department of Home Affairs (the department) from 18 to 19 February 2019. We made **nine suggestions** as a result of the inspection and sent the department a report outlining our findings on 15 May 2019.

Table 7 – Stored communications inspection statistics: Department of Home Affairs

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	27	24 (89%)
Stored communications warrants	14	14 (100%)
Destruction of stored communications information	7	7 (100%)

Progress since previous inspection
Over previous inspection periods we identified, and the department has disclosed, serious compliance issues relating to its use of stored communications powers. However, the scale and seriousness of these issues decreased as the department

developed and implemented measures to improve its compliance.

Significant findings

Lack of awareness regarding the stored communications provisions of the Act

The department disclosed four warrants issued by an AAT member, where the department provided an accompanying affidavit but did not provide a written application for the warrant to the issuing authority, contrary to s 111 of the Act. This occurred due to a lack of staff awareness and clarity regarding the department's stored communications process, including the absence of relevant instructions or guidelines.

We suggested the department undertake education initiatives to address this knowledge gap. At the time of our inspection the department was drafting stored communications procedures and developing new systems. In response to our findings, the department advised that it was reviewing its training materials and delivering targeted awareness-raising sessions.

Historic preservation notices given in a successive manner

The department disclosed that it gave a total of 15 historic domestic preservation notices in a successive manner. We previously advised the department that giving successive historic domestic preservation notices in such a manner, covering the same carrier and person or service, is akin to giving an ongoing domestic preservation notice, which the department cannot authorise because it is not an interception agency. The department advised our Office it has ceased this practice.

Stored communications warrants applied for and exercised, and stored communications received, by unauthorised persons

The department disclosed that officers who were not authorised to do so under ss 110(3) and 135(2) of the Act had applied for, and received stored communications under four stored communications warrants. In addition, we identified that an officer who was not authorised to do so under s 127 of the Act had exercised the authority of these warrants.

We suggested the department ensure it keeps operational areas informed of changes to delegations, nominations or authorisations. The department advised it is committed to ensuring officers understand the powers they are exercising under the Act and it would act to remediate its educational and procedural arrangements.

Directing carrier to undertake action it is not required to take or does not have lawful authority to perform

We identified two warrants where the department had not received discs containing requested stored communications from the carrier and they were otherwise unable to be located. The department had requested that the carrier retain the preserved stored communications until a new warrant could be sought.

The Act does not require carriers to retain communications once a historic domestic preservation notice ceases to be in force. We identified that the department's request to the carrier, that it keep communications in this manner, may have led the carrier to believe that it was required to do so under law.

We suggested the department cease directing carriers to undertake actions that it is not required, or does not have lawful authority, to perform under the Act. The department acknowledged our advice and stated that it will ensure its instructions to carriers reflect this position.

Accessed stored communications not made or received by the person named on the warrant

Section 117 of the Act states that a stored communications warrant authorises access to stored communications made or intended to be received by the person specified on the warrant, subject to any conditions or restrictions on the warrant. We identified one instance where the department obtained a warrant in the name of the person subscribed to the service number, rather than the person under investigation who was using the number. As the service was not being used by the subscriber, the stored communications the department accessed were not made or intended to be received by the person named on the warrant, contrary to the requirements under s 117 of the Act.

In addition to making a suggestion about managing the stored communications it had received, we also suggested that, where it has evidence that a service is subscribed in one name but being used by a different person who is under investigation, the department should specify the person under investigation on the warrant. The department advised that it would implement training and procedural updates to address this issue.

Table 8 – Inspection findings: Department of Home Affairs

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Warrants applied for without a written application	-	4	1 suggestion	s 111
Warrants applied for, authority of warrants exercised, and stored communications received by unauthorised persons	4	4	1 suggestion	s 110, s 127, s 135
Directing carrier to undertake action it is not required to take or does not have lawful authority to perform	1	-	1 suggestion	s 107H(1), s 107K, s 108(2)(f)

Accessed stored communications not made or received by the person named on the warrant	1	-	2 suggestions	s 117
Warrant mistakenly left to expire	-	1	-	s 119(1)
Unlawfully accessed stored communications not identified	1	-	1 suggestion	s 119(1)
Warrant not in the prescribed form	1	-	-	s 118(1)(a), Form 6
Has the agency properly managed accessed stored communications?				
Destruction conducted under an implied authorisation	1	-	1 suggestion	s 150(1)
Missing information in reporting to the Minister	2	-	1 suggestion	s 150(2)
Has the agency properly applied the preservation notice provisions?				
Giving historic domestic preservation notices in a successive manner	-	15	-	s 107H(1)(b)(i), s 107J(1)(a)(ii)
Has the agency satisfied certain record-keeping obligations?				
Compliance with record-keeping obligations	-	3	-	s 151(1)(h), s 151(1)(c)
Other findings				
Unable to assess stored communications information	2	-	1 suggestion	-
No records to evidence the compliance process for stored communications	-	4	-	-

5. Independent Commissioner Against Corruption (South Australia)

We inspected the ICAC (SA) from 22 to 23 November 2018. We made **one suggestion** as a result of the inspection and sent the ICAC (SA) a report outlining our findings on 12 December 2018.

Table 9 – Stored communications inspection statistics: Independent Commissioner Against Corruption (South Australia)

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	1	1 (100%)
Ongoing domestic preservation notices	8	8 (100%)
Stored communications warrants	2	2 (100%)

Progress since previous inspection

At our 2017–18 inspection of the ICAC (SA) we identified two issues that required remedial action. These issues were not identified again at this inspection and we were satisfied with the action that the ICAC (SA) had taken to address our earlier findings.

We did not make any significant findings at the 2018–19 inspection.

Table 10 – Inspection findings: Independent Commissioner Against Corruption (South Australia)

Issue	**Identified**	**Disclosed**	**Suggestion/ Recommendation**	**Section of Act**
Is the agency only dealing with lawfully accessed stored communications?				
Warrant not in the prescribed form	2	-	1 suggestion	s 118(1)(a), Form 6
Has the agency properly applied the preservation notice provisions?				
Preservation notices not revoked	-	4	-	s 107L(2)(a)(ii)

6. New South Wales Police Force

We inspected the New South Wales Police Force (NSWPF) from 8 to 11 October 2018. We made **one suggestion and one better practice suggestion** as a result of the inspection and sent the NSWPF a report outlining our findings on 11 December 2018.

Table 11 – Stored communications inspection statistics: New South Wales Police Force

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	458	51 (11%)
Ongoing domestic preservation notices	100	9 (9%)
Stored communications warrants	405	56 (14%)
Destruction of stored communications information	122	122 (100%)

Progress since previous inspection

During our 2017–18 inspection, we identified an instance where stored communications were destroyed without chief officer approval, contrary to s 150(1) of the Act. We identified further instances of this issue during our 2018–19 inspection.

Significant findings

Stored communications warrant applied for in relation to a victim of a serious contravention

We identified one instance where the NSWPF applied for a stored communications warrant to access the stored communications of a victim of a serious contravention without their consent. Based on the information the NSWPF provided in the accompanying affidavit, it was our view that the NSWPF could have sought the victim's consent. We also identified this issue during our 2017–18 inspection of the NSWPF's compliance with Chapter 3 of the Act.

Destruction of stored communications information

In three instances, the NSWPF did not destroy stored communications information 'forthwith' as required under s 150(1) of the Act. This was evident as, during our inspection, we located copies of stored communications information that had been certified for destruction. However, we were satisfied that the NSWPF destruction processes were sound and these instances appeared to be the result of human error.

Based on disclosures the NSWPF made to us during the inspection, we also identified two instances where stored communications were destroyed without chief officer approval, contrary to the requirements under s 150(1) of the Act. Our discussions with staff indicated that the NSWPF's actions in these instances were undertaken in response to an error by a carrier and were aimed at managing stored communications information appropriately. The NSWPF advised us it had reminded staff of their obligations under s 150(1) of the Act.

Table 12 – Inspection findings: New South Wales Police Force

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Stored communications warrant applied for in relation to a victim of a serious contravention	1	-	-	s 116(1)(da)
Unlawfully accessed stored communications not identified and quarantined	1	-	-	s 117, s 118(2)
Unable to determine whether stored communications were lawfully accessed	4[13]	-	1 suggestion	s 117
Inconsistencies in applications and warrants	3	-	-	s 112(b), s 118(1)(a), Form 6
Template wording in supporting affidavits	General finding	-	1 better practice suggestion	s 113
Has the agency properly managed accessed stored communications?				
Stored communications not destroyed 'forthwith'	3	-	-	s 150(1)
Stored communications information destroyed without chief officer approval	2	-	-	s 150(1)

7. Queensland Police Service

We inspected the QPS between 6 and 8 August 2018. We made **two suggestions** as a result of the inspection and sent the QPS a report outlining our findings on 16 October 2018.

Table 13 – Stored communications inspection statistics: Queensland Police Service

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	45	9 (20%)
Ongoing domestic preservation notices	243	41 (17%)
Stored communications warrants	147	45 (31%)
Destruction of stored communications information	119	42 (35%)

[13] This is the number of warrants affected by this issue, not the number of stored communications for which we were unable to determine whether the information was lawfully accessed.

Progress since previous inspection
At our 2017–18 inspection, we noted instances where information was not destroyed 'forthwith' in accordance with s 150(1) of the Act and others where stored communications information was destroyed prior to being certified by the chief officer. We identified similar destruction-related issues at this inspection.

Significant findings
Destruction of stored communications information
At this inspection we noted inconsistencies in the QPS's processes that ultimately affected its ability to destroy stored communications information forthwith as required by s 150(1) of the Act.

We identified instances where stored communications information was not destroyed forthwith, instances where copies of stored communications were retained after being certified for destruction, records that indicated stored communications were destroyed prior to certification by the chief officer and instances where it was unclear whether destruction had taken place.

We suggested the QPS establish clear guidelines for staff on its destruction processes to ensure destructions are conducted in a timely and consistent manner. The QPS advised that it implemented new processes to remediate its approach to destroying stored communications information.

Table 14 – Inspection findings: Queensland Police Service

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Has the agency properly managed accessed stored communications?				
Destruction of stored communications information	General finding	-	1 suggestion	s 150(1)
Inaccuracies in reporting to the Minister	1	-	1 suggestion	s 150(2)

8. Tasmania Police

We inspected Tasmania Police from 22 to 26 October 2018. We made **two recommendations** about its overall approach to compliance (as discussed in **Part B** of this report), and made **two recommendations, 10 suggestions and one better practice suggestion** specifically about its access to stored communications. We sent Tasmania Police our final report on 16 July 2020.

Table 15 – Stored communications inspection statistics: Tasmania Police

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	3	3 (100%)
Ongoing domestic preservation notices	37	21 (57%)
Stored communications warrants	35	23 (66%)
Destruction of stored communications information	39	25 (64%)

Progress since previous inspection

During our 2018–19 inspection, we identified that Tasmania Police had not taken sufficient remedial action to address findings from our 2017–18 inspection. This led us to identify broader issues relating to Tasmania Police's awareness of the requirements under Chapter 3 of the Act, and the mechanisms and processes it has in place to support compliance.

Significant findings

Insufficient remedial action taken for previous inspection findings

We identified instances where Tasmania Police had not taken sufficient remedial action in response to suggestions we made following our 2017–18 inspection. For example, at our 2017–18 inspection we identified instances of stored communications warrants Tasmania Police had issued in relation to victims of serious contraventions in circumstances where the victim did not consent or was not provided with the opportunity to consent. Although the relevant investigations appeared not to have been progressed, we were not satisfied that Tasmania Police had fully acted on our previous suggestions and we made further suggestions to Tasmania Police regarding this issue. Tasmania Police advised us about action it has taken in response to our suggestions, including updating its standard operating procedures.

We identified two instances at our 2017–18 inspection where a carrier provided Tasmania Police with stored communications that did not comply with the warrant conditions. During our 2018–19 inspection, we found that Tasmania Police had not taken any action to manage the information it received from the carrier under these two warrants. Due to the risks posed by these issues, in our 2018–19 inspection report we recommended to Tasmania Police that it establish clear and effective procedures for accessing and disseminating stored communications accessed under warrants subject to conditions or restrictions, including assessing whether the stored communications information provided by a carrier is consistent with the authority of the warrant. Tasmania Police advised us it made changes in line with our recommendation, but we remain of the view that further procedural guidance is required.

Destruction of stored communications information
We identified issues affecting Tasmania Police's destruction processes, including:

- a lack of contemporaneous records to indicate when stored communications were destroyed, to demonstrate that destruction took place forthwith in accordance with s 150(1) of the Act
- instances where, at the time of the inspection, stored communications information certified for destruction was not destroyed
- stored communications information which was not certified for destruction by the chief officer until approximately one year after it was identified as no longer being required
- instances where stored communications were destroyed without chief officer approval. (We identified this issue previously in our 2017–18 inspection and identified it again during this inspection period. However, these instances were all dated prior to our 2017–18 inspection and were present in this sample due to the retrospective nature of our inspections.)

We suggested that, in order to remediate the inconsistencies in its destruction practices, Tasmania Police should establish clear guidelines for its staff on destruction processes. This should assist Tasmania Police in ensuring that destructions are conducted in a timely and consistent manner in accordance with s 150 of the Act.

Tasmania Police told us it amended its destruction processes and updated its standard operating procedures.

Non-compliant processes for receiving stored communications
At both the 2017–18 and 2018–19 inspections, we identified that all stored communications a particular carrier provided to Tasmania Police were received by a staff member who was not authorised to receive them under s 135(2) of the Act. This meant that a key part of the stored communications process was performed by a staff member who had no training or guidance on the requirements of Chapter 3 of the Act. This, in turn, presented risks to Tasmania Police's management of stored communications and its ability to account for using and communicating this information.

We recommended that Tasmania Police establish a mechanism to ensure that it appropriately and accountably receives stored communications in accordance with s 135(1) and (2) of the Act. In response to our recommendation, Tasmania Police told us it has since ceased this practice and now all stored communications are sent directly to an area where all staff are covered by the s 135(2) authorisation.

Management of unlawfully accessed stored communications
We identified instances where an ineligible issuing authority invalidly issued stored communications warrants. We were not satisfied that Tasmania Police had taken appropriate remedial action to manage the unlawfully accessed stored

communications or that there was sufficient awareness within Tasmania Police of the existence of these invalid warrants.

To ensure that Tasmania Police can identify when unlawfully accessed stored communications are received and manage such information appropriately, we suggested it establish clear protocols to confirm that stored communications returned by the carrier comply with the warrant. Tasmania Police has advised they would update its standard operating procedures.

Annual reporting to the Minister

We identified that, at the time of our inspection, Tasmania Police had not provided its annual report to the Minister for the 2017–18 period, contrary to s 159 of the Act. We suggested Tasmania Police provide its 2017–18 annual report to the Minister and update its standard operating procedures to ensure staff are aware of the reporting obligations under the Act. Tasmania Police advised our Office that it would include reporting obligations in its procedures.

Table 16 – Inspection findings: Tasmania Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Stored communications warrants applied for in relation to a victim of a serious contravention	2[14]	-	2 suggestions	s 116(1)(da)
Management of unlawfully accessed stored communications	6[15]	-	1 suggestion	-
Warrants not in prescribed form	General finding	-	-	s 118(1)(a), Form 6
Inconsistencies in warrants	General finding	-	1 better practice suggestion	s 118(1)(a) Form 6
Has the agency properly managed accessed stored communications?				
Destruction of stored communications information	General finding	-	2 suggestions	s 150(1)(b), s 151(1)(i)
Non-compliant processes for receiving stored communications	General finding	-	1 recommendation	s 135(2)

[14] Originally identified during our 2017–18 inspection.
[15] Including four instances initially identified in the 2017–18 inspection.

Has the agency properly applied the preservation notice provisions?				
Preservation notices not revoked	-	6	-	s 107L(2)(a)(ii)
Wording regarding the basis for giving historic domestic preservation notices	3	-	1 suggestion	s 107M(1)(a)
Has the agency satisfied certain record-keeping obligations?				
Annual reporting to the Minister	-	1	2 suggestions	s 159
Was the agency cooperative and frank?				
No remedial action taken on non-compliance with stored communications warrant conditions	2[16]	-	1 recommendation 2 suggestions	s 117

9. Victoria Police

We inspected Victoria Police from 25 to 27 February 2019. We made **one suggestion and four better practice suggestions** as a result of the inspection and sent Victoria Police a report outlining our findings on 15 March 2019.

Table 17 – Stored communications inspection statistics: Victoria Police

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	38	12 (32%)
Ongoing domestic preservation notices	111	31 (28%)
Stored communications warrants	90	36 (40%)
Destruction of stored communications information	50	22 (44%)

Progress since previous inspection

We did not identify any compliance issues as a result of our 2017–18 inspection. However, at our inspection in 2016–17 we identified instances where Victoria Police had applied to access the stored communications of a victim of a serious contravention without obtaining their consent. We identified this issue again at our 2018–19 inspection.

Significant findings

Warrants issued by an ineligible authority

We identified three warrants that were issued by an AAT member who was not appointed under s 6DB(1) of the Act to issue stored communications warrants. We

[16] Originally identified during our 2017–18 inspection.

note that Victoria Police were not the only agency affected by this issue during 2018–19 and acknowledge Victoria Police was unaware the AAT member was not appointed at the time the warrants were issued.

While we were engaging with the AAT in relation to instances identified at Victoria Police, Victoria Police contacted us to advise it had become aware the member was not an eligible authority. Victoria Police disclosed that, during this inspection period, the member issued Victoria Police with a total of 17 stored communications warrants. Victoria Police advised it had taken action in line with our suggestions to manage the stored communications it obtained under these warrants.

Stored communications warrants applied for in relation to a victim of a serious contravention

We identified two instances where Victoria Police applied for and obtained a stored communications warrant to access the stored communications of a victim of a serious contravention. Following the inspection, Victoria Police advised that the staff involved in the first instance were given instructions to prevent the issue recurring. For the second instance, Victoria Police acknowledged our Office's view that it should not have sought to access the victim's stored communications, but submitted that it was open to the issuing authority to grant the warrant. At our next inspection we will review the legal advice Victoria Police obtained regarding this second instance.

Table 18 – Inspection findings: Victoria Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Warrants issued by an ineligible authority	3	17[17]	1 suggestion	s 110(1), s 5(1), s 6DB(1)
Stored communications warrants applied for in relation to a victim of a serious contravention	2	-	-	s 116(1)(da)
Not establishing the link between the telecommunications service and the person specified on the warrant	1	-	1 better practice suggestion	s 113, s 117

[17] This includes three warrants identified by our Office during the inspection. Victoria Police also advised of at least 24 stored communications warrants issued by the ineligible authority for the 2018–19 inspection at the time, which we will assess during our next inspection.

Has the agency properly managed accessed stored communications?				
Recording the time of destruction where records are destroyed on the same date as certification	General finding	-	1 better practice suggestion	s 150(1), s 151(1)(l)
Has the agency properly applied the preservation notice provisions?				
Risk identified where a preservation notice is given for two telecommunications services used by different people	1	-	1 better practice suggestion	s 107H(3)
Inconsistency in the offence details on preservation notices	General finding	-	1 better practice suggestion	s 107J(1)(b), s 5E(1)
Other findings				
Unable to assess stored communications received	9	-	-	s 117 s 150(1)
Minor administrative issue: Transposing errors on documents	2	-	-	-

10. Western Australia Police

We inspected the WA Police from 8 to 11 October 2018. We did not make any recommendations or suggestions as a result of the inspection and sent the WA Police a report outlining our findings on 1 February 2019.

Table 19 – Stored communications inspection statistics: Western Australia Police

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	35	7 (20%)
Ongoing domestic preservation notices	44	11 (25%)
Stored communications warrants	26	18 (69%)

Progress since previous inspection

Most of the issues we identified at our 2017–18 inspection of the WA Police were not identified at our 2018–19 inspection.

At our 2017–18 inspection we identified instances where preservation notices were left to expire and we were unable to determine whether the WA Police had complied with the mandatory revocation requirements under s 107L(2)(a)(ii) of the Act. At this inspection, we identified one preservation notice that expired in similar circumstances. However, the WA Police demonstrated improved compliance in this area and has since advised us it had made changes to its standard operating procedures to assist it in meeting the mandatory revocation requirements.

No significant issues were identified at this inspection.

Table 20 – Inspection findings: Western Australia Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Has the agency properly applied the preservation notice provisions?				
Preservation notices not revoked	1	-	-	s 107L(2)(a)(ii)

Part D—Telecommunications data

Telecommunications data and the oversight function of the Commonwealth Ombudsman

Since amendments to the Act on 13 October 2015, our Office has had an overarching role in assessing agencies' compliance with Chapter 4 when using the telecommunications data powers.

Telecommunications data is information about an electronic communication, which does not include the content or substance of that communication. A stored communications or telecommunications interception warrant is required if an agency seeks the content of a communication.

Telecommunications data includes, but is not limited to:

- subscriber information (for example, the name, date of birth and address of the person to whom the service number is subscribed)
- the date, time and duration of a communication
- the phone number or email address of the sender and recipient of a communication
- the Internet Protocol (IP) address used for the session
- 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 (this may be at a single point in time, or at regular intervals over a period of time).

Agencies can internally make an authorisation for the disclosure of telecommunications data under Chapter 4 of the Act. There are different types of authorisations that enable agencies to access either existing information or documents (known as a historic authorisation), or future information or documents for a limited period[18] (known as a prospective authorisation). However, if an agency wishes to access telecommunications data that will identify a journalist's source, the agency must apply to an external issuing authority for a warrant.

Only officers authorised by the chief officer of the agency can authorise the disclosure of telecommunications data. Once the authorisation is made, it is notified to a carrier, which then provides the information to the agency.

There are various considerations that must be made before an agency can authorise disclosure of telecommunications data. These considerations involve weighing the perceived utility and relevance of the disclosed data to the investigation against the privacy intrusion it will cause. The Act also sets out requirements for the form of authorisations and notifications, as well as specifying how and for what purposes telecommunications data can be used or communicated.

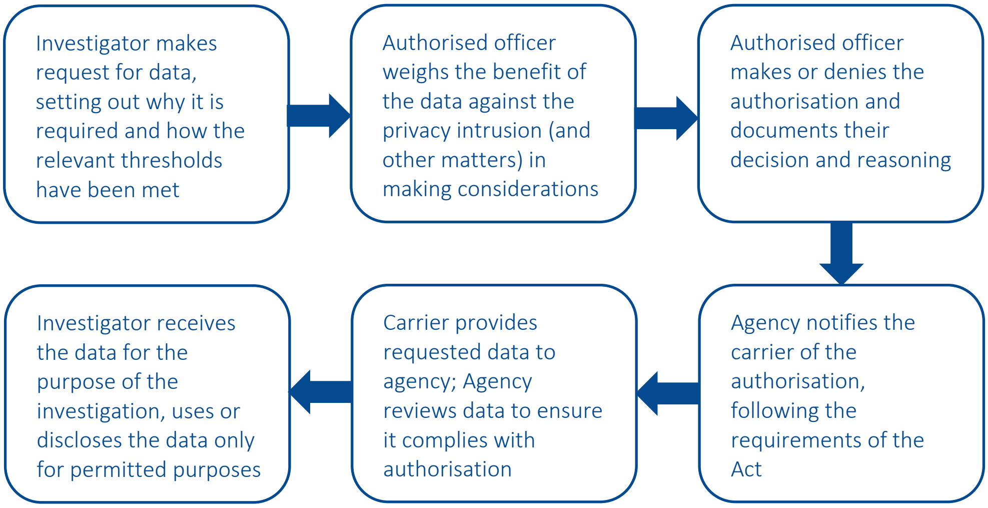
[18] Maximum 45 days from when the authorisation is made (s 180(6)(b) of the Act).

Our Office does not review the merits of decisions to authorise disclosing data. However, we carefully consider whether agencies are satisfying the requirements of the Act, with a particular focus on confirming officers authorising these disclosures have sufficient information to make the required considerations.

Unlike covert powers used under Chapters 2 and 3 of the Act, the decision to authorise the intrusion into somebody's privacy is made by the agency investigating, rather than an external issuing authority. Therefore, it is important that agencies can demonstrate that they are making the required considerations to provide assurance their intrusive and covert powers are being used appropriately.

To demonstrate this, it is crucial that agencies have good record-keeping practices. Our Office's role is to provide assurance to the Parliament and public that agencies are using their powers appropriately and, in the absence of sufficient records, we cannot provide this assurance.

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



Our inspections involve inspecting a sample of records for both historic and prospective authorisations. We look at the background material in the request documents, to check – in line with s 180F of the Act – that authorised officers had enough information before them to make the required considerations.

We assess the processes agencies have in place to make authorisations, notify the carriers and manage the data once it is received. By closely inspecting a sample of individual records in detail, alongside the processes, guidance and general approach of an agency to complying with the Act, we can gain a detailed understanding of an agency's overall compliance with the Act.

Since our oversight function of telecommunications data regime commenced in 2015, our approach to assessing compliance with Chapter 4 has developed and matured. We now have a better understanding of how the legislation operates in practice, the challenges agencies face in using it in a manner consistent and compliant with the Act, and how we can provide critical and constructive feedback to agencies on their different approaches to it.

Summary of telecommunications data findings

During 2018–19, our Office inspected 10 agencies' access to telecommunications data, covering records made from 1 July 2017 to 30 June 2018. Following the inspections it was evident that, while some agencies were able to demonstrate a high level of compliance with the Act, others still had work to do. In some instances the retrospective nature of our inspections meant the issues related to records that had already been made, but were not yet due to be assessed, at the time of our previous inspection. However, in other instances agencies had not taken sufficient action to address our previous compliance findings.

The table below sets out each agencies' use of the Chapter 4 powers during the period and highlights that certain agencies have much higher usage than others. We identified that many agencies have substantial room for improvement in developing consistent procedures to adequately satisfy the requirements of the Act. We also identified that – alongside processes, training and guidance to staff – a culture where compliance is valued is vital to ensuring these powers are being used as legislated.

Most agencies were receptive to our findings, recommendations and suggestions.

Table 21 – Use of telecommunications data powers and records that were inspected at agencies in the 2018–19 period

Agency	Total Historic	Historic Inspected	Total Prospective	Prospective Inspected	Total inspected
ACIC	7,498	34	1,401	44	78
AFP[19]	19,549	61	3,700	61	155
ASIC	1,896	41	17	13	54
CCC (QLD)	1,271	59	203	48	107
Home Affairs	3,639	61	264	50	111
NSW Police	98,604	62	1044	60	122
QLD Police	25,273	67	3430	67	134
Tasmania Police	9,194	62	175	30	92
Victoria Police	82,723	63	9,686	62	125
WA Police	25,107	62	1521	60	122

[19] These figures do not accurately reflect the number of authorisations made. The reasons for this are discussed further in the body of the report.

Additionally, the Australian Federal Police was issued Journalist Information Warrants (JIWs) and made authorisations for telecommunications data on behalf of foreign countries.

Table 22 – Australian Federal Police use of JIWs and authorisations made for telecommunications data on behalf of foreign countries and records that were inspected in the 2018–19 period:

JIWs	JIWs Inspected	Foreign Historic	Foreign Historic Inspected	Foreign Prospective	Foreign Prospective Inspected	Total inspected
6[20]	-	65	30	1	3[21]	33

Agencies not inspected in relation to Chapter 4 of the Act in the 2018–19:

As a result of the risk-based approach applied by our Office in 2018–19, we did not inspect all agencies' compliance with Chapter 4 of the Act (see **Part A**). Agencies that we did not inspect were the:

- Australian Competition and Consumer Commission
- Australian Commission for Law Enforcement Integrity
- Corruption and Crime Commission Western Australia
- Independent Broad-based Anti-corruption Commission
- Law Enforcement Conduct Commission
- New South Wales Crime Commission
- Independent Commission Against Corruption (New South Wales)
- Northern Territory Police
- Independent Commissioner Against Corruption (South Australia)
- South Australia Police.

Where we did not inspect an agency in 2018–19, a sample of the relevant records (authorisations that ceased to be in force between 1 July 2017 and 30 June 2018) were inspected in 2019–20 and the results will be included in our 2019–20 annual report.

Compliance issues and compliance risks

There were a number of common issues that were identified at most agencies we inspected in 2018–19. This section includes a brief overview of these issues and the compliance risks they create for agencies. More detail on the specific circumstances at each agency can be found in the telecommunications data findings section. These issues continue to present risks to an agency's ability to meet compliance with the Act and the Office's ability to conduct inspections. We continued to monitor these issues closely at our 2019–20 inspections.

---

[20] Authorisations made under these JIWs were inspected during the September 2018 non-routine inspection of the AFP which followed up on the earlier 2017 breach of the JIW provisions by the AFP. See https://www.ombudsman.gov.au/__data/assets/pdf_file/0034/96748/A-report-on-the-Commonwealth-Ombudsmans-inspection-of-the-Australian-Fe....pdf.

[21] Only one foreign prospective authorisation was reflected in the statistics provided to our Office. The other foreign prospective authorisation (which was extended once, which we have counted as a separate instance) was identified at the inspection.

Demonstration of required considerations when making a decision to authorise disclosure of telecommunications data

Before deciding to make an authorisation disclosing telecommunications data under the Act, authorised officers must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from disclosing or using the telecommunications data is justifiable and proportionate.[22] Agencies must also keep documents or other materials that indicate an authorisation was properly made, including that all relevant considerations have been made.[23]

The Act sets out the considerations an authorised officer must have regard to in weighing up whether the privacy intrusion is justified and proportionate, being:

- the relevance and usefulness of the data to the investigation
- the seriousness of the offence under investigation
- the reason why the disclosure is sought – this involves considering, for example, whether the agency has already tried other, less intrusive methods.

At five of the 10 agencies we inspected in 2018–19, we identified instances where we were unable to assess whether the authorised officer had enough information available to them at the time of making the authorisation to be satisfied that disclosure of the data was justified and proportionate.

In some instances this may have been because the authorised officer was orally briefed at the time of application or was directly involved in the investigation. However, without records of this, we could not be satisfied the required considerations were made.

Many agencies include standardised wording in their authorisation template that states the authorised officer has made the considerations under the Act, but we do not consider template wording alone is sufficient to meet this requirement.

[22] See s 180F of the Act for more detail of what considerations are required.

[23] Section 186A(1)(a)(i) of the Act requires the chief officer 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. In considering 'other materials', we may rely on an agency's policies and procedures, systems checks and interviews with relevant officers of the agency to inform our understanding of an agency's processes, which we then use to assess the agency's compliance with this section.

Case Study 3— Australian Federal Police

During our inspection of the AFP, we identified multiple telecommunications data requests that did not include detailed background information, or referred only to case numbers or operations. This made it difficult for us to assess whether an authorised officer was provided with sufficient information, especially as, in many instances, the authorised officer had also not kept particular records of their decision-making. The sorts of records we would expect to see 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.

Based on our inspection, we concluded the AFP's authorised officers did not have a consistent practice for documenting their considerations made 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 Act.

We recommended that the AFP implement processes to ensure authorised officers consistently document any information relevant to considering and approving a telecommunications data authorisation under Chapter 4 of the Act, 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) of the Act.

Telecommunications data accessed without proper authority

We identified instances at all inspections in 2018–19 where agencies had accessed telecommunications data without proper authority. As such, the disclosure of the data was unauthorised. For example, as a result of administrative error, the agency stated the wrong service number or time period on an authorisation, or entered the wrong number into the Integrated Public Number Database (IPND).

In other instances there were defects in the authorisation process, such as no valid authorisation being in place or authorisations that were made by officers who were not delegated to do so.

There were a small number of instances where authorisations were made orally; a practice which is not provided for by the Act. The individual tables of inspection findings under each agency summary below identify where this occurred.

Data not available: unable to assess compliance

At some agencies, we inspected records where we were unable to assess compliance with the Act because the relevant telecommunications data was not made available. This can be due to the technical difficulties of retrieving data from systems the agency uses to manage sensitive information or because it has been destroyed on the basis that it is no longer required for an investigation. If we cannot access the data, we cannot verify that the data the agency received was within the scope of the authorisation, or provide assurance to the Parliament and the public that the powers are being used appropriately.

Although there is no express legislative provision requiring agencies to retain received telecommunications data in their records, s 186B(2)(b) of the Act entitles the Ombudsman to full and free access to all records relevant to an inspection once notification is provided under s 186B(3) of the Act. In order for our Office to assess compliance, it is essential that agencies retain received telecommunications data until we have had the opportunity to review the associated records.

Data received outside the parameters of the authorisation

At all agencies, we identified instances where carriers had provided data that was not authorised because it was outside the parameters of the authorisation. This included instances where the carrier provided data that exceeded the time period authorised, or provided a different type of data than was authorised.

While many agencies have processes for identifying and quarantining unauthorised data, at around half of our inspections we identified further instances (beyond those picked up by agencies' quality assurance processes) where carriers had provided data that was outside the parameters of the authorisation. This indicates a need for continued training and improved processes for identifying and managing any data carriers provide that is not authorised.

Insight into our telecommunications data inspections

How we assess that telecommunications data disclosed by the carrier, and used by the agency, complies with an authorisation

In some instances carriers may provide additional information that the agency did not specifically authorise. When this occurs, we expect the agency to identify and quarantine the data from any use or disclosure.

To assess agencies' ability to do this, we review individual records and examine each agency's processes and procedures to guide staff on identifying data that may not be within the parameters of the authorisation.

We also undertake our own assessments of the data that has been received when inspecting the records of authorisations that fall within our sample.

We assess the data received by the agency to confirm it:

- is within the parameters of the authorisation, including for the correct service number and within the relevant timeframe specified on the authorisation
- is the type of data that has been authorised for disclosure by the agency
- does not contain the content of the communication.

Example of how we identify whether data is inside the parameters of an authorisation:

Example parameters	
Authorised Number	0491 570 006[24]
Authorised Data	Call charge records
Period Authorised	1/07/2018 to 30/06/2019
Date Authorised	30/06/2019 1300 (AEST)
Sent to Carrier	30/06/2019 1400 (AEST)

Example results			
Line	**Date and Time**	**Caller**	**Recipient**
1	30/06/2018 2100 (UTC)	0491 570 006	0491 570 156
2	01/07/2018 0300 (UTC)	0491 570 006	0491 570 156
3	01/07/2018 0900 (UTC)	0491 570 156	0491 570 006
…			
10	30/06/2019 0359 (UTC)	0491 570 006	0491 570 156
11	30/06/2019 0500 (UTC)	0491 570 006	0491 570 156

Our Assessment	
1	This line is within the parameters of the authorisation as conversion from UTC to AEST means this call occurred at 01/07/2018 0700 AEST. Note: as the authorisation does not state a time zone for the period authorised, it is taken to apply the time zone of the location in which it was made.
2	This line is within the parameters authorised.
3	This line is not authorised, as the authorisation only related to calls made by the mobile phone number, not calls received by this number.
10	This line is authorised, as after conversion to AEST, it occurred at 30/06/2019 1359, before the time the authorisation was notified to the carrier.
11	This line is not authorised, as it is after the time the authorisation was notified to the carrier (0500 UTC is 1500 AEST on the same day).

For these results, it is our expectation that the agency proactively identified and quarantined the unauthorised data (e.g. lines 3 and 11) before results were disseminated to an investigator. Where this unauthorised information is not

[24] The phone numbers provided in this table are derived from a list of numbers provided by the Australian Communications and Media Authority (ACMA) for use in publications. They are not real mobile telephone numbers.

identified before being sent to investigators, we suggest the agency contact any recipients and quarantine the data. We would also suggest that the agency ascertain whether use or disclosure has taken place and take appropriate actions to address any potential ramifications.

Findings from telecommunications data inspections conducted in 2018–19

Our key findings for the 10 inspections we completed during 2018–19 are summarised below. This does not include all issues or findings we raised with the agency.

After receiving our inspection report, agencies often tell us about remedial action they have taken in response to our inspection findings. We review the effectiveness of these actions at our subsequent inspections and include our findings in the appropriate annual report.

1. Australian Criminal Intelligence Commission

We inspected the ACIC from 6 to 29 November 2018. We made **eight suggestions** as a result of the inspection and sent the ACIC a report detailing our findings on 16 January 2019.

Table 23: Telecommunications data inspection statistics: Australian Criminal Intelligence Commission

Telecommunications data authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	7,498	34 (0.45%)
Prospective	1,401	44 (3.14%)

Progress since previous inspection

At our 2017–18 inspection we highlighted several issues that required remedial action. Although we identified a small number of these issues again at this inspection, we were satisfied that the ACIC was taking sufficient action to address these.

The ACIC consistently demonstrates thorough preparation for our inspections, and proactively discloses instances of non-compliance and associated remedial actions. This is reflective of strong quality assurance and disclosure procedures.

Significant findings

The ACIC disclosed 171 instances where telecommunications data was accessed without proper authority, which occurred as acting arrangements for the relevant authorised officers had not been formalised.

We suggested to the ACIC that they take further steps to confirm the nature of the acting arrangements in place at the time the authorisations were made, including whether the appointments were made by an appropriate person and prior to the relevant authorisations being made. The ACIC advised its commitment to improving the training and control mechanisms around these processes to ensure those acting in authorised officer positions are formally authorised before fulfilling the authorised functions.

The ACIC disclosed seven instances where it accessed telecommunications data without a signed authorisation in place. The ACIC disclosed four instances of prospective authorisations where formal approval was not documented by the authorised officer and nine instances where the relevant authorisation was not made prior to the telecommunications data being requested from the carrier.

For these instances, we suggested the ACIC quarantine the affected data from further use or disclosure. In response the ACIC advised that, in all instances, either no information was received or all relevant information was quarantined.

Table 24 – Inspection findings: Australian Criminal Intelligence Commission

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Telecommunications data accessed without proper authority				
Authorised officers not formally acting in authorised position	-	171	1 suggestion	s 5AB(1)
No authorisation made	-	7	1 suggestion	s 178(2), s 180(2), s 183
No authorisation prior to request for telecommunications data		9	1 suggestion	
Formal approval of authorisation not recorded (unsigned)		4		
Formal approval of revocation of authorisation not recorded (unsigned)[25]		2		
Telecommunications data received for service not listed on authorisation[26]	1	-	1 suggestion	s 178(2), s 180(2)

[25] For the two instances where authorisations were unsigned, the ACIC noted it has implemented updates to systems to minimise the ability for unsigned authorisations to be sent to a carrier.

[26] The authorisation stated reference numbers, rather than the specific telecommunications service. On request, the ACIC advised the carrier of the service to be searched; however, this was not specified on the authorisation.

Telecommunications data outside parameters of authorisation				
Historic telecommunications data received under prospective authorisation[27]	2	-	1 suggestion	s 178(2), s 180(2)
Telecommunications data received after expiry of prospective authorisation	1	1		
Telecommunications data dated after time of notification (historic authorisation)	1	-		
Telecommunications data outside date range specified[28]	-	3		
Telecommunications data received after revocation took effect	2	7	1 suggestion	s 180(7)
Other findings				
Authorisation sent to carrier not specified on authorisation	1	1	2 suggestions	s 181B(1) s 181B(3)
Incorrect reporting of authorisations made[29]	1	-	-	s 186
Transposing error[30]	1	-	-	s 183(f) s 183(2)
Form of authorisations and revocations[31]	5	-	-	s 183

2. Australian Federal Police

We inspected the AFP from 11 to 15 February 2019. We made **one recommendation and eighteen suggestions** to the AFP and sent the AFP a report outlining our findings on 5 August 2020. Due to the delay in finalising this report, it also included comments on the AFP's progress based on our more recent 2019–20 inspection. The full results of that inspection will be included in our 2019–20 annual report.

[27] The ACIC advised that quarantining was not required as in one instance the parameters were correct, and no data was received in the other instance.

[28] One of these instances occurred as a result of the carrier retuning telecommunications data in a different time zone to that used on the authorisation. The other two instances were a result of the ACIC notifying the incorrect authorisation parameters to the carrier. There were also an additional 19 instances, where the ACIC identified that the carrier had provided telecommunications data outside the period authorised, which demonstrated that the ACIC generally had effective procedures for identifying such occurrences.

[29] In this instance, a prospective authorisation was reported under s 186 of the Act as a historic authorisation.

[30] The incorrect service number was listed on the notification of the authorisation. No telecommunications data was accessed, however, there was a risk that the ACIC could have received telecommunications data that was not authorised.

[31] These were isolated errors relating to information that was required to be stipulated on an authorisation, but was incorrectly stated. There was no substantive issue with the ACIC's templates identified.

Table 25 – Telecommunications data inspection statistics: Australian Federal Police

Telecommunications data authorisations		
Type of records	**Records made available**[32]	**Records inspected**
Historic	19,549	61 (0.31%)
Prospective	3,700	61 (1.65%)
Foreign historic	65	30 (46.15%)
Foreign prospective	1	1 (100%)

Progress since previous inspection

At the 2017–18 inspection, our Office was not satisfied that the AFP authorised officers demonstrated that they consistently had regard to the considerations required under the Act, and we 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*.

At our 2018–19 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 this recommendation.

We also identified several instances where we could not confirm the authorised officer had made the required considerations before authorising the disclosure of telecommunications data. This resulted in a further recommendation, below.

Significant findings

Many requests for authorisations made by requesting officers did not include detailed background information, or referred only to case numbers or operations and, as such, we were not able to assess what information the authorised officer had regard to in making the authorisation. The absence of a consistent practice among authorised officers of documenting their considerations when making an authorisation meant we had a general lack of confidence that authorised officers routinely had regard to the required considerations.

[32] These figures do not accurately reflect the number of authorisations made. The reasons for this are discussed further in the body of the report.

Due to the ongoing nature of the issue, we made the following recommendation:

> The Australian Federal Police implement 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).

We also identified that the AFP had made two foreign prospective authorisations[33] (one of which had been extended) in the absence of the Attorney-General having made an authorisation under s 15D of the *Mutual Assistance in Criminal Matters Act 1987*, despite this being required before a foreign prospective authorisation can be made. In our 2019–20 inspection, we found that the AFP was not able to account for the use and disclosure of the information it obtained under one of these authorisations and suggested that it do so.[34] The AFP has since updated its procedures and established protocols for seeking s 15D authorisations.

We identified two foreign historic authorisations the AFP had made where content[35] was provided by the carrier. The AFP then disclosed the content to the requesting country. There were also four foreign historic authorisations made by the AFP that authorised the disclosure of content. However, the carrier did not provide any content.

For all of these authorisations, the AFP retained the wording of the original request from the foreign law enforcement country, without verifying whether the request was permitted by the Act.

We made four suggestions regarding foreign authorisations: two specifically in relation to managing the disclosure of content to the foreign law enforcement agency, one regarding training for officers involved in the foreign authorisation process and one about the need for further review of such authorisations to ensure officers do not request content.

[33] Only one foreign prospective authorisation was reflected in the statistics provided to our Office. The other foreign prospective authorisation (which was extended once, and which we have counted as a separate instance) was identified on inspection.
[34] The AFP advised that it quarantined the data and the data was not disclosed.
[35] Telecommunications data does not include the substance or content of a communication. To provide content, a carrier must be given a telecommunications interception warrant (Chapter 2 of the Act) or stored communications warrant (Chapter 3 of the Act).

Table 26 – Inspection findings: Australian Federal Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorisation process				
Demonstration of authorised officer considerations	General finding	-	1 recommendation[36]	s 180F s 186A(1)(a)(i)
Foreign Authorisation Issues				
Foreign prospective authorisations made without proper authority and telecommunications data received under an invalid authorisation	3	-	1 suggestion	s 180B(2) s 180B(3)(a) s 180B(3)(b)
Foreign authorisation for content, content disclosed to foreign law enforcement agency	2	-	4 suggestions[37]	s 172
Foreign authorisation requesting content, no content received	4	-		
Amendments affecting validity of authorisations[38]	General finding	-	2 suggestions[39]	s 183
Telecommunications data accessed without proper authority				
Incorrect service authorised for disclosure	2	-	2 suggestions	s 180F
Oral authorisation	-	2	1 suggestion	s 183
Authorisation not in required form	2	-		s 183
Data not available: unable to assess compliance[40]	-	1	1 suggestion	s 186A(1)(g)

[36] The AFP advised that in November 2019 it provided instructions for authorised officers to use a free-text field implemented in the request form to document their considerations for historic authorisations and also made changes to its prospective authorisation templates to enable authorised officers to do the same.

[37] In response to our suggestion, the AFP advised it quarantined the data. The AFP also advised that it incorporated these instances into its training, including a step by step document outlining areas of risk identified during the inspection.

[38] These authorisations were amended by requesting officers after being signed by the authorised officer. There is no mechanism in the Act that provides for amendments without approval by the authorised officer.

[39] The AFP advised it altered its internal processes so that any amendment to the authorisation forms requires re-authorisation.

[40] In one instance, the AFP destroyed data prior to our inspection. Although there is no legislative requirement for data to be retained by the agency, the absence of such records meant our Office was unable to assess whether the data was within the parameters of the authorisation. In response to our suggestion, the AFP advised it would update

Journalist information warrants				
Consideration of journalist information requirements[41]	23	-	2 suggestions [42]	s 180H
Demonstration that information relevant to considering journalist information requirements was made available to authorised officer[43]	2	-	1 suggestion[44]	s 180H
Telecommunications data outside parameters of authorisations				
Telecommunications data outside parameters	-	4	2 suggestions[45]	s 178(2)
Telecommunications data post-revocation[46]	-	3	-	s 180(7)
Other findings				
Authorisations not reflected in statistics provided to our Office	4	-	1 suggestion[47]	s 186
Statistics did not reflect authorisations made[48]	General finding	-	1 suggestion	-
Erroneous use of revocation provision[49]	-	1	-	s 180(7)
Foreign prospective authorisations not in required form	-	General finding	1 suggestion[50]	s 183(1)(f)
Court statement request recorded against disclosure provisions[51]	-	1	1 suggestion	s 185A

its destruction processes to include a quality assurance check to ensure any prospective data has been inspected by our Office prior to destruction.

[41] The AFP's prospective authorisation template requires the requesting officer to answer a question about whether the request related to journalist information. No answer was stated in these 23 instances. Our two suggestions related to re-incorporating this question (as it was removed following the inspection) and uniformly considering journalist information requirements across all authorisations.

[42] The AFP advised it amended its prospective authorisation forms.

[43] While detailed consideration had been given to journalist information requirements, there was nothing to demonstrate that this consideration had been shared with the authorised officer.

[44] In response to our suggestion, the AFP advised it will incorporate this in training as an example of the types of supporting documentation that a requesting officer is required to bring before an authorised officer.

[45] In addition to a suggestion that AFP quarantine unauthorised data, we also suggested that the AFP considers the risk of receiving unauthorised data when data is received in a time zone different to that stated on the authorisation. In response to our suggestion, the AFP advised that the authorised officer would be made aware that a carrier might return ancillary information not necessarily specified in the authorisation.

[46] This was as a result of a legacy process, which has since been amended.

[47] The AFP advised that it adjusted its internal reporting and would issue an addendum to the Minister for Home Affairs.

[48] Our Office requires an agency to report all authorisations it makes, regardless of whether or not they are notified to a carrier. This enables us to assess issues that prevent an authorisation being progressed.

[49] The AFP advised it updated its revocation processes.

[50] The AFP provided its foreign prospective authorisation template to our Office for feedback.

[51] The AFP advised this was an isolated incident and it has guidance on this issue in its standard operating procedures.

Administrative errors in categorisation of authorisation	-	3	-	-

3. Australian Securities and Investments Commission

We inspected ASIC on 14 November 2018. We made **two suggestions** and sent ASIC a report outlining our findings on 11 December 2018.

Table 27 – Telecommunications data inspection statistics: Australian Securities and Investments Commission

Telecommunications data authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	1,898	41 (2.16%)
Prospective	17	13 (74.5%)

Progress since previous inspection

At our 2017–18 inspection we identified four issues that required remedial action. At our 2018–19 inspection we were satisfied ASIC had taken appropriate remedial action on all but one of these issues.

Significant findings

ASIC disclosed 28 instances[52] where officers who were no longer authorised to do so had made telecommunications data authorisations. This occurred because ASIC had prepared a new authorisation instrument under s 5AB(1) of the Act which deliberately omitted a number of officers who were previously authorised. It appears these changes were not sufficiently communicated within ASIC and a number of officers who were not included on the new instrument continued to make authorisations in the belief they were authorised. ASIC took appropriate remedial action to quarantine all telecommunications data received as a result of these unauthorised disclosures.

We suggested ASIC consider ways to communicate more effectively any future changes to s 5AB authorisation instruments.

[52] Three of these relate to the 2019–20 inspection period; however, given the timing of the inspection, will be reported here.

Table 28 – Inspection findings: Australian Securities and Investments Commission

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Telecommunications data accessed without proper authority				
Officer not authorised to make authorisations	-	28	1 suggestion	s 5AB
Incorrect service number notified to carrier[53]	-	2	-	s 178(2) s 180(2)
Telecommunications data outside parameters of authorisations				
Telecommunications data received after expiry of prospective authorisation[54]	3	-	1 suggestion	s 180(2)
Other findings				
No record of when notification of authorisation occurred[55]	4	-	-	s 186A(1)(a)(iii)
Form of prospective authorisations[56]	General finding	-	-	s 183
Form of revocations[57]	General finding	-		

4. Crime and Corruption Commission (Queensland)

We inspected the CCC (Qld) from 21 to 24 January 2019. We made **10 suggestions** and sent the CCC (Qld) a report outlining our findings on 4 June 2019.

Table 29 – Telecommunications data inspection statistics: Crime and Corruption Commission (Queensland)

Telecommunications data authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	1,271	59 (4.64%)

[53] No suggestion was made, as ASIC identified and quarantined the affected data. We were satisfied these were isolated instances.

[54] ASIC had specified an expiry date on the authorisation which was earlier than intended, which contributed to it receiving telecommunications data which came into existence after the authorisation had expired. These records fell within the next inspection period, but as they were disclosed by ASIC at the time of the inspection they were included within this period.

[55] ASIC's standard practice at the time was to record these times in a spreadsheet, which was not followed in these instances.

[56] This template omitted the short particulars of the offence as required by the s 183 Determination. These omissions were addressed by ASIC during the inspection.

[57] This template omitted three elements, including the time on which the revocation was made. These omissions were addressed by ASIC during the inspection.

Prospective	203	48 (23.65%)

Progress since previous inspection
At our 2017–18 inspection we identified four issues that required remedial action. At our 2018–19 inspection we were satisfied with the remedial action the CCC (Qld) had taken in relation to two of the issues, but we concluded that there were still issues with the form of templates, as well as instances where data was received after an authorisation was revoked. We made suggestions to the CCC (Qld) to address these issues.

Significant findings
We identified that the CCC (Qld)'s processes placed the obligation on requesting officers to demonstrate that the required considerations had been made under the Act, rather than on the authorised officer. We also identified errors on authorisations that indicated a lack of appropriate consideration by authorised officers. We suggested the CCC (Qld) review its policies and procedures to ensure it is able to demonstrate that authorised officers consistently have regard to the required considerations. The CCC (Qld) has amended its templates to remove the obligation on requesting officers to demonstrate that the required considerations have been made. At our 2019–20 inspections, we engaged with the CCC about implementing processes to demonstrate that the authorised officer has had regard to the relevant considerations. This will be discussed in our 2019–20 annual report.

We made three suggestions to the CCC (Qld) about its processes for authorisations and revocation of authorisations, as well as its authorisation templates. These suggestions were aimed at improving the consistency of the CCC (Qld)'s processes which will support its ability to demonstrate compliance with the Act.

At our inspection we encountered a system limitation that prevented the CCC (Qld) from retaining the telecommunications data it had received. This meant that, for one telecommunications data type authorised for disclosure, we were unable to assess whether the results complied with the parameters of the authorisation. There is no express legislative requirement for an agency to retain received telecommunications data in its records; however, without this data we were unable to complete our assessments. The CCC (Qld) promptly implemented system changes to ensure that the data is retained for longer.

Table 30 – Inspection findings: Crime and Corruption Commission (Queensland)

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorisation Process				
Records to demonstrate whether an authorisation was properly made[58]	14	-	-	s 186A(1)(a)
Difficulty determining scope and authority of authorisation[59]	1	-	1 suggestion	-
Demonstration of privacy considerations	6	-	1 suggestion	s 180F s 186A(1)(a)(i)
Difficulty determining when revocation of an authorisation took effect	5	-	1 suggestion	s 180(6) s 180(7)
Partial revocation of authorisations[60]	1	1	-	180(6) 180(7)
Telecommunications data accessed without proper authority				
Searches conducted on service not explicitly listed on authorisation[61]	-	3	2 suggestions	s 183
Unauthorised additional access to telecommunications data [62]	-	2	1 suggestion	s 178(2)
Telecommunications data outside parameters of authorisations				
Telecommunications data received after revocation took effect	2	7	1 suggestion	s 178(2) s 180(2)
Telecommunications data outside parameters of authorisation	3	-	2 suggestions	

[58] In these instances, we had identified issues with duplicate electronic signatures on authorisations, inconsistencies in using signature fields for inserting of electronic signatures and missing actions in record-keeping audit trails due to system issues.
[59] The CCC (Qld) had a legacy 'folio' process where additional authorisations could be made against the originating request. In this instance, this process created ambiguity as to what had been authorised. The CCC (Qld) has since revised its practices to improve the clarity and scope of authorisations, including establishing new templates.
[60] Although a prospective authorisation may request more than one data type, and agencies may wish to cease receiving one data type but continue to receive another, there is no mechanism to revoke only a component of the authorisation i.e. partially revoke an authorisation.
[61] The authorisations referred to searches on service numbers, but did not include the specific telecommunications service. This was part of a process for bulk searches of the IPND, where the CCC (Qld) would attach the services to be searched to the authorisation. However, this process was not followed and there was no link between what was authorised and the services searched.
[62] This was one instance where additional unauthorised searches were conducted using the results of an authorised search as the search parameters (cascading searches). We suggested the CCC (Qld) quarantine these additional results and seek advice on these searches.

Other findings				
Telecommunications data unavailable – unable to assess compliance	General finding	-	-	-
Required record not kept - no record of when notification of authorisation occurred[63]	1	-	-	s 86A(1)(a)(iii)
Form of authorisations	General finding	-	1 suggestion	s 183 Determination
Form of revocations		-		
Transposing error in authorisation	-	2	-	1
Statistical and reporting issues[64]	4	3	-	s 186

5. Department of Home Affairs

We inspected the Department of Home Affairs (the department) from 15 to 19 October 2018. We made **two suggestions** as a result of the inspection and sent the department a report outlining our findings on 30 November 2018.

Table 31 – Telecommunications data inspection statistics: Department of Home Affairs

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	3,639	61 (1.7%)
Prospective	264	50 (18.9%)

Progress since previous inspection

At our 2017–18 inspection, we identified that, due to limitations in the department's telecommunications data request system, the department had received telecommunications data from a carrier which was outside the date range specified on the authorisation. We identified this again at our 2018–19 inspection, when the department disclosed 54 similar instances.

Significant findings

The department disclosed 74 instances where an officer who was not authorised to do so under s 5AB(1) of the Act[65] made authorisations for telecommunications data.

[63] We were satisfied this was an isolated instance, as it is the CCC (Qld)'s usual practice to keep these records.

[64] These instances related to the manner in which the CCC (Qld) categorised authorisations. For example, in one instance an authorisation reported as authorising a single type of telecommunications data, was identified as having authorised two types. This likely occurred as a result of the legacy folio system complicating the CCC (Qld)'s process for keeping statistics on authorisations.

[65] Subsection 5AB(1) of the Act states that the chief officer of an enforcement agency may authorise, in writing, a management officer or management position to be an 'authorised officer'. Only an authorised officer may authorise the disclosure of telecommunications data.

This occurred as the department had introduced a new authorisation instrument under s 5AB(1) of the Act that increased the level of seniority required of authorised officers. The department did not communicate the change effectively to its staff, therefore the officer continued to make authorisations despite no longer being authorised to do so. We were satisfied the officer had acted in good faith, believing they remained authorised.

We suggested the department consider ways to more effectively communicate changes to its s 5AB authorisations. The department advised that it would consider ways to communicate these changes and share information between different areas of the agency. The department also took appropriate remedial action, including quarantining all unauthorised telecommunications data and disclosing the issue to our Office.

The department disclosed 54 instances where it received telecommunications data that was outside the period specified on the authorisation. In the course of our inspection we identified an additional seven instances.

In each instance the department's telecommunications data request system inputted the end time for authorisations as 00:00, rather than 23:59, which meant the period of the authorisation ended at the beginning of the day rather than the end. While the department sought to address this through manual annotations on the authorisations, in some instances telecommunications data disclosed was dated after the end time of the authorisation and therefore outside of what was authorised.
We suggested the department quarantine all affected telecommunications data from further use or disclosure, pending the outcome of internal advice it had sought. The department informed our Office that it had done so.

Table 32 – Inspection findings: department of Home Affairs

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Telecommunications data accessed without proper authority				
Officer not authorised to make authorisations	-	74	1 suggestion	s 5AB(1)
Telecommunications data outside parameters of authorisation				
Telecommunications data outside date range specified	7	54	1 suggestion	s 178(2) s 180(2)
Other issues				
Revocation of an authorisation not in correct form[66]	General finding	-	-	-
Historic authorisation not in correct form[67]	9	-	-	s 183 Determination

6. New South Wales Police Force

We inspected the NSWPF from 30 July to 2 August 2018. We made **one recommendation and two suggestions** as a result of the inspection and sent the NSWPF a report outlining our findings on 26 October 2018.

Table 33 – Telecommunications data inspection statistics: New South Wales Police Force

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	98,604	62 (0.06%)
Prospective	1,044	60 (5.75%)

Progress since previous inspection

At our 2016–17 inspection, we identified the NSWPF's Counter Terrorism and Special Tactics Command's (CTSTC) standard practice was to provide verbal authority for searches of the IPND. We provided the NSWPF with our findings from that inspection in June 2018, which highlighted the requirement in s 183 of the Act that authorisations for access to telecommunications data be in either written or electronic form and signed by the authorised officer.

[66] The basis on which the department is a criminal law-enforcement agency was incorrectly stated (s 176A rather than 110A of the Act). The department updated the template when we advised of this error.

[67] This related to authorisations where the disclosure of historic telecommunications data was sought from multiple carriers. In these instances, the authorisation did not state all carriers from whom the disclosure was sought, as required by the s 183 Determination.

We suggested that the NSWPF review its policies and procedures to ensure all authorisations for disclosure of telecommunications data are in written or electronic form and signed by the relevant authorised officer, in accordance with s 183 of the Act.[68]

Significant findings

At our 2018–19 inspection we identified that the NSWPF's CTSTC's practice of providing oral authority for IPND searches had continued until the end of July 2018. The NSWPF advised it had recently updated its processes to ensure IPND searches are only conducted after an authorised officer has provided a written approval; however, this process had not been implemented at the time of our inspection. We identified that, in certain circumstances, the Telecommunications Interception Branch (TIB) was conducting IPND searches and obtaining subscriber telecommunications data without a written or electronic authorisation in place.[69] As a result of the inaction following our previous suggestion, we made the following recommendation:

> That the New South Wales Police Force should review its policies and procedures to ensure all authorisations for telecommunications data are in written or electronic form and signed by the relevant authorised officer, in accordance with section 183 of the Act.

The NSWPF adopted this recommendation.

In 30 instances we were unable to assess whether telecommunications data the NSWPF had received was within the parameters of the relevant authorisations. The NSWPF's archiving process for prospective authorisations meant there was a delay in the data being made available to us to inspect.[70] Although we acknowledged the technical difficulties, we expressed concern that the NSWPF's archiving practice may continue to impede our access to records and encouraged it to consider ways to make these records more readily available.[71] We reviewed these records during our subsequent inspection, the results of which will be included in our 2019–20 annual report.

[68] In response to the streamlined report, the NSWPF reviewed the oral authorisations, located staff notes, but did not locate authorisations that were in written or electronic form and signed by the relevant authorised officer in accordance with the Act. The NSWPF did not provide further comments to our suggestion.

[69] Some operational staff may have incorrectly interpreted telecommunications data access authorisations to have a 'cascading effect' to permit disclosure of further telecommunications data with a lower perceived level of intrusion despite not being specified in the authorisation.

[70] The NSWPF's practice is to archive telecommunications data received from carriers under prospective authorisations after three months and where use or disclosure is no longer required.

[71] In response to our report, the NSWPF reinforced its commitment to comply with its obligations under the Act and advised that it will continue to engage with our Office on this issue.

Table 34 – Inspection findings: New South Wales Police Force

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Telecommunications data accessed without proper authority				
Oral authorisation	General	-	1 recommendation	s 183
Telecommunications data outside parameters of authorisation				
Telecommunications data outside date range specified	1	-	1 suggestion	s 178(2)
Period authorised inconsistent to request	1	-	1 suggestion	s 178(2)
Other issues				
Telecommunications data unavailable	30	-	-	-
No revocation of authorisation when no longer required[72]	1	-	-	s 180(7)

7. Queensland Police Service

We inspected the QPS from 10 to 14 December 2018. We made **three suggestions** as a result of the inspection and sent the QPS a report outlining our findings on 27 March 2019.

Table 35 – Telecommunications data inspection statistics: Queensland Police Service

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	25,273	67 (0.27%)
Prospective	3,430	67 (1.95%)

Progress since previous inspection

At our 2017–18 inspection we identified four issues that required remedial action. Based on our 2018–19 inspection we were satisfied the QPS had taken appropriate action on these issues.

Significant issues

In one instance we were unable to assess whether telecommunications data the QPS had received complied with the authorisation for a locations-based dataset. The QPS's systems only retained the data for 30 days which meant it was not available to us at the time of our inspection. There is no express legislative requirement for received telecommunications data to be retained in an agency's records. However, without this data we were unable to complete our assessments.

[72] In this instance, there was correspondence available that indicated the authorised officer was satisfied the disclosure was no longer required. Despite this, there was no indication that the authorisation had been formally revoked in line with s 180(7) of the Act.

We suggested to the QPS that it review its approach to retaining this dataset to ensure our ability to assess its compliance at future inspections.[73]

We identified that the QPS had made an authorisation requesting access to content, which is not permitted under the Act. The carrier did not provide content in response to this authorisation and the QPS advised it was creating additional guidance for its staff to avoid a recurrence of this issue.

Table 36 – Inspection findings: Queensland Police Service

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Telecommunications data accessed without proper authority				
Authorisation requesting access to content[74]	1	-	-	s 172
Telecommunications data accessed without proper authority – transposing error	1	-	-	s 178(2)
Telecommunications data outside parameters of authorisation				
Telecommunications data outside the parameters of an authorisation	1	3	-	s 178(2) s 180(2)
Authorisation Process				
Privacy considerations not demonstrated by records[75]	2	-	-	s 180F s 186A(1)(a)(i)
Standard approval process not followed[76]	1	-	-	s 183 s 180F

[73] Although this related to one authorisation, this issue would have affected our inspection of any authorisation made for this dataset, making this finding general in nature. In response to the streamlined report, the QPS noted that discussions were underway to increase the scope of retention for this dataset.

[74] No suggestion was made to the QPS as this appeared to be an isolated instance and it was improving guidance on this issue.

[75] In one of these instances, there was no documentation on the authorised officer's decision making. In the other, the authorised officer had not completed a decision making checklist, which meant that we were unable to form a view that the authorised officer had made the required considerations. However, in discussing this with the authorised officer we were able to be satisfied of the authorised officer's awareness of the considerations to be made.

[76] We were unable to confirm that the authorised officer was involved in making the authorisation. Specifically, there was no email trail to establish that the authorised officer had inserted their electronic signature on the authorisation, which is contrary to the QPS practices.

Other issues				
Authorisation made for longer than permitted period[77]	3	-	-	s 180(2) s 180(6)(b)(i)
Telecommunications data unavailable	1	-	1 suggestion	s 186A(1)(g)
Revocation issue[78]	1	-	1 suggestion	s 180(6) s 180(7)
Multiple authorisations assigned a single reference[79]	1	-	1 suggestion	s 186
Authorisation not in required form[80]	1	-	-	s 183 Determination

8. Tasmania Police

We inspected the Tasmania Police from 22 to 26 October 2018. We made **two recommendations**, **10 suggestions and one better practice suggestion** as a result of the inspection. We also made **two recommendations** to the Tasmania Police about its overall approach to compliance (as discussed in **Part B** of this report).

We provided our final report to the Tasmania Police on 16 July 2020. Due to the delay in finalising the report, it also included comments about the Tasmania Police's progress based on the results of our 2019–20 inspection, held in November 2019. The results of that inspection will be included in our 2019–20 annual report.

Table 37 – Telecommunications data inspection statistics: Tasmania Police

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	9,194	62 (0.67%)
Prospective	175	30 (17%)

Progress since previous inspection

At our 2017–18 inspection, we highlighted several issues that required remedial action. At this inspection, we were not satisfied the Tasmania Police had implemented sufficient measures to improve compliance, particularly in relation to:

[77] These three authorisations were made for a period of 46 days — one day longer than permitted by s 180(6)(b)(i) of the Act. These authorisations were made out of hours and were subsequently revoked without any data being received outside the permitted period.
[78] It appeared the carrier had not fully revoked this authorisation. Due to the issue with the retention of telecommunications data for this particular dataset, we were unable to confirm that the QPS had ceased to receive data after revocation.
[79] This may have resulted in underreporting to the Minister on the number of authorisations made.
[80] This was an isolated instance as we did not identify issues with the QPS' authorisation templates.

- demonstrating that authorised officers made the required considerations when making authorisations
- properly making authorisations for disclosures from the Integrated Public Number Database (IPND)
- determining when historic authorisations were notified to carriers
- telecommunications data being received after authorisations were revoked.

Significant findings

In making an authorisation for telecommunications data, the authorised officer must be satisfied of the relevant considerations including the privacy consideration under s 180F of the Act. For historic authorisations (excluding IPND authorisations) we identified that these considerations were being made by regional investigators rather than the authorised officer. As such we were not satisfied that the authorised officer had personally made the required considerations.

There were no records to demonstrate what information was available to the authorised officer at the time of authorisation. We are aware that agencies often rely on oral briefings to support authorised officers' understanding of an investigation and associated decision making. However, when these discussions were not formally documented, we could not be satisfied the Tasmania Police had achieved compliance with the requirement to ensure records are kept to demonstrate an authorisation has been properly made. For this reason, we made the following recommendation to the Tasmania Police:

> Tasmania Police establish procedures to ensure authorised officers demonstrate the required considerations when authorising access to telecommunications data under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*.

Subsequent to our 2018–19 inspection Tasmania Police introduced a new authorisation workflow, which we assessed during our 2019–20 inspection.[81] While this was a positive step toward addressing our recommendation, there are additional steps that could be taken to more clearly demonstrate whether an authorised officer has made the required considerations, including placing a stronger emphasis on the requirement for authorised officers to make contemporaneous records of the basis for their decisions.

We identified that, for the majority of disclosures from the IPND, the Tasmania Police did not have written or electronic authorisations in place. Although some records indicated that certain steps in the authorisation process had taken place (such as a requesting officer documenting approval from the authorised officer), no written authorisation had generally been made. Without this, the requirements of s 183 of

[81] This decentralised the authorisation process, where regional inspectors now make the authorisations, rather than a single designated position at the Tasmania Police. Our full assessment of the Tasmania Police's progress will be set out in the 2019–20 Annual Report.

the Act were not met. Any disclosure of telecommunications data without a valid written authorisation is unauthorised and should be quarantined. As a result, we made the following recommendation:

> Tasmania Police should review its policies and procedures to ensure all authorisations for telecommunications data are in written or electronic form and signed by the relevant authorised officer, in accordance with s 183 of the *Telecommunications (Interception and Access) Act 1979*.

We suggested that, where a valid, written authorisation was not in place, the Tasmania Police quarantine any results disclosed from the IPND. We also made several suggestions that Tasmania Police quarantine unauthorised data or data outside the parameters of authorisation. At our 2019–20 inspection the Tasmania Police could not demonstrate that the quarantining we suggested had taken place.

Table 38 – Inspection findings: Tasmania Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorisation Process				
Considerations not demonstrated for historic authorisations (excl. IPND)	General finding	-	1 recommendation	s 180F s 186A(1)(a)(i)
Considerations not demonstrated - IPND	General finding	-		
Authorisations not in written form for disclosures from IPND	General finding	-	1 recommendation, 1 suggestion	s 183
Telecommunications data accessed without proper authority				
Authorisations not for permitted purpose[82]	8	-	1 suggestion	s 178
Telecommunications data not specified on authorisation received	2	-	1 suggestion	s 178 s 178A s 179
Telecommunications data after time of notification	1	-	1 suggestion	

[82] An authorisation for access to historic information under s 178 of the Act must not be made by an authorised officer unless satisfied the disclosure is reasonably necessary for enforcing the criminal law, which is a 'permitted purpose.' These authorisations did not specify a criminal offence and only included a statement that they related to 'coronial matters', despite the authorisations being made under s 178 of the Act.

Telecommunications data outside parameters of authorisation				
Telecommunications data received after revocation took effect[83]	3	-	2 suggestions	s 180(2) s 180(7)
Other issues				
Annual report not completed	General finding	-	2 suggestions	s 186
No records to demonstrate when authorisation notified to carrier	General finding	-	1 suggestion	s 186A(1)(a)(iii)
Typographical errors	3	-	-	-
IPND requests did not meet form requirements	General finding	-	1 suggestion	s 183 Determination
Authorisations not revoked when no longer required[84]	2	-	1 better practice suggestion	s 180(7)

9. Victoria Police

We inspected Victoria Police from 1 to 3 October 2018. We made **three recommendations and five suggestions** and sent Victoria Police a formal report outlining our findings on 23 April 2019.

Table 39 – Telecommunications data inspection statistics: Victoria Police

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	82,723	63 (0.08%)
Prospective	9,686	62 (0.64%)

Progress since previous inspection

At our 2017–18 inspection we identified five issues that required remedial action. Based on our 2018–19 inspection we were satisfied Victoria Police had taken appropriate remedial action on two of those issues. For the remaining three, we noted that:

- Despite Victoria Police advising us it had posted prominent guidance for staff that authorisations must not request the substance or content of a communication, we were not able to easily locate this guidance.

[83] We suggested that the Tasmania Police quarantine this data and also undertake to ascertain use and disclosure of information that was provided to investigators that was received after the revocation took effect.

[84] Despite information indicating the disclosure was no longer required, there was nothing to indicate that the authorised officer had been advised of these circumstances which means the authorisations were not revoked (when an authorised officer may have made such a decision).

- Victoria Police was unable to action our suggestions that it quarantine certain telecommunications data because its system did not have a mechanism to limit access to telecommunications data (this is discussed further below).
- Victoria Police's system does not automatically apply the legislative limit for duration of prospective authorisations. We did not identify any records that were affected by this system limitation, but consider it remains a risk to compliance.

Significant findings

We identified the authorisations processed by the team at Victoria Police that is responsible for the bulk of historic authorisations lacked background information to substantiate requests for access to telecommunications data. We also identified an absence of records to indicate that authorised officers had made the relevant considerations before making an authorisation.[85] For this reason we made the following recommendation:

> That Victoria Police implements processes to ensure authorised officers demonstrate the required considerations when authorising access to telecommunications data under s 180F of the *Telecommunications (Interception and Access) Act 1979.*

We identified that the area of Victoria Police that processes the bulk of its authorisations did not have training or reference materials in place to guide its staff in accessing telecommunications data. We consider that awareness and training are important controls contributing to an agency's compliance with the Act. Although Victoria Police advised it was seeking approval to create a formal training package, given the lack of progress on our previous suggestions,[86] we made the following recommendation:

> That Victoria Police reviews its approach to awareness raising and training about telecommunications data to ensure all staff involved in exercising telecommunications data powers have a thorough understanding of the legislative framework and their responsibilities under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*.

[85] This contrasted with other areas of Victoria Police (that processed a smaller volume of authorisations) where authorisations were often detailed and accompanied by checklists to demonstrate that the required considerations had been made.

[86] Most recently, following the 2017–18 inspection, we suggested that Victoria Police provide targeted training to authorised officers regarding what can be authorised for disclosure under the Act, and that it review its policies and procedures to ensure officers are fully informed of the requirements of the Act.

Where an agency receives telecommunications data that is not covered by an authorisation (for example, where data is outside the parameters specified on the authorisation), the agency is responsible for ensuring that this data is appropriately managed. In our view such data should be quarantined from further use or disclosure. Victoria Police advised that its RMS system[87] does not have the ability to quarantine (i.e. limit access) telecommunications data. As this presents an ongoing compliance risk, we made the following recommendation:

> That Victoria Police implements processes to prevent use or disclosure of unauthorised telecommunications data under Chapter 4 of the *Telecommunications (Interception and Access) Act 1979.*

Table 40 – Inspection findings: Victoria Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorisation Process				
Considerations not demonstrated	General finding	-	1 recommendation	s 180F s 186A(1)(a)(i)
No process to revoke authorisations[88]	General finding	-	1 suggestion	s 180(7)
Telecommunications data accessed without proper authority				
Authorisations not for permitted purpose[89]	1	-	1 suggestion	s 178 s 178A s 179
Officer not authorised to make authorisations[90]	-	1	1 suggestion	s 5AB
Telecommunications data outside parameters of authorisation				
Telecommunications data outside data parameters on authorisation	1	-	1 suggestion	s 178(2)

[87] This is the system used to process the vast majority of authorisations at Victoria Police.
[88] We identified that no authorisations were revoked by one area of Victoria Police and there was no process in place for revoking authorisations. We considered the lack of this process, coupled with there being no mandatory training for officers in this area, presented a risk to compliance and could result in unnecessary privacy intrusion.
[89] An authorisation for access to historic information must be made for a 'permitted purpose', set out in ss 178, 178A, and 179 of the Act. In this instance, the authorisation had not been made for a permitted purpose, and we suggested Victoria Police seek legal advice on using authorisations for this purpose.
[90] Subsection 5AB(1) of the Act states that the chief officer of an enforcement agency may authorise, in writing, a management officer or management position to be an 'authorised officer'. Only an authorised officer may authorise the disclosure of telecommunications data. In this instance, a prospective authorisation was given by an officer not formally acting in a position covered by the s 5AB authorisation.

Other issues				
Insufficient training and awareness	General finding	-	1 recommendation	-
No ability to quarantine telecommunications data	General finding	-	1 recommendation	-
Use and disclosure risks[91]	General finding	-	1 suggestion	-
Data not available: unable to assess compliance	-	1	-	s 186A(1)(g)
Authorisations did not meet form requirements	General finding	-	-	s 183 Determination
	1	-	-	

10. Western Australia Police

We inspected the WA Police from 8 to 11 October 2018. We made **five suggestions** and sent the WA Police a report outlining our findings on 15 November 2018.

Table 41 – Telecommunications data inspection statistics: Western Australia Police

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	25,107	62 (0.25%)
Prospective	1,521	60 (3.94%)

Progress since previous inspection

We were satisfied that the WA Police had taken adequate remedial action to address the four issues we raised during our last inspection.

Significant findings

We identified one instance where the WA Police accessed telecommunications data without a written or electronic authorisation signed by an authorised officer. As there was no authorisation in place, we advised the WA Police that the access was not authorised and suggested the telecommunications data should be quarantined.

[91] We identified that, although Victoria Police's RMS system has an audit log to track use and disclosure, officers are able to download results from RMS and any use and disclosure would not be captured by the inbuilt audit function. This presents a risk that use and disclosure would not be captured in line with the Act.

Table 42 – Inspection findings: Western Australia Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Telecommunications data accessed without proper authority				
No written or electronic authorisation in place	1	-	1 suggestion	s 183
Telecommunications data not specified on authority[92]	1	-	1 suggestion	s 178(2) s 180(2)
Telecommunications data outside parameters of authorisation				
Telecommunications data outside date range specified	3	-	1 suggestion	s 178(2) s 180(2)
Telecommunications data received after revocation[93]	2	-	2 suggestions	s 180(7)

[92] The carrier provided two data types, one was not specified on the authorisation. The WA Police had received reverse call charge records (where the target phone number is dialled) when it had only requested call charge records (where the target phone number dials another number). This authorisation had been raised to capture data that was not received under a prospective authorisation. In response to the report, the WA Police noted it considers the additional data was lawfully obtained. We advised that should the WA Police wish to rely on the original prospective authorisation, quarantining was still necessary, as not all data was covered by that authorisation.

[93] The first instance occurred as a result of a delay between when the revocation took effect and it being provided to the carrier. The second instance was a result of an incorrect date applied to a revocation causing it to come into effect earlier than intended.

Part E— Glossary

Term (and section of the Act)	Description
AAT	Administrative Appeals Tribunal
Access a stored communication s 6AA	For the purpose of this Act, accessing a stored communication consists of listening to, reading or recording such a communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication.
Administrator of the *Telecommunications (Interception and Access) Act 1979*	Following the *Administrative Arrangements Order – amendment made 1 February 2020*, the Minister for Home Affairs is responsible for administering the 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 or warrant. 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.
Affidavit	A written statement confirmed by oath or affirmation, for use as evidence in court.
AGD coversheet	When providing stored communications to an agency, the carrier will typically complete an AGD "*Response to a stored communications warrant issued under the Telecommunications (Interception and Access) Act 1979*" coversheet. This document outlines important dates and times as recorded by the carrier, including when it accessed the stored communications on its systems.
Appointment of approving officers to exercise the authority of stored communications warrants s 127	Under s 127(1) of the Act, the authority conferred by a stored communications warrant may only be exercised by a person in relation to whom an approval under s 127(2) is in force in relation to a warrant. Under s 127(2) of the Act, the chief officer of a criminal law-enforcement agency, or an officer in relation to whom an appointment under s 127(3) of the Act is in force, may approve a person to exercise the authority conferred by warrants or classes of warrants. We interpret exercising the authority of the warrant to be the act of providing the warrant to the carrier with a request for the carrier to release the stored communications to the agency.

Authorisation for access to telecommunications data ss 178-180B and s 183	An authorisation for access to telecommunications data under Chapter 4 of the Act permits the disclosure of information or documents by a carrier 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 Act, agencies may authorise the disclosure of specified information or documents that come into existence during the period for which the authorisation is in force, if satisfied that the disclosure is reasonably necessary for investigating a serious offence (as defined in s 5D) 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 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 Act. Under s 180B of the Act, the AFP can authorise disclosure of specified information or documents that come into existence during the period for which the 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 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; or give, or revoke, an ongoing preservation notice or a foreign preservation notice (the AFP only) under the Act. In addition to the specified positions set out in the definition of authorised officer under s 5 of the Act, the head of an enforcement agency may, by writing, authorise a management office or management position in the enforcement agency as an authorised officer (s 5AB(1)). 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	When referred to 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.
Conditions and restrictions s 118(2)	A stored communications warrant may specify conditions or restrictions relating to accessing stored communications under the warrant.
Conditions for giving preservation notices s 107H(2) and s 107J(1), s 107N(1) and s 107P	Under s 107H(2) of the Act, a criminal law-enforcement agency may only give a domestic preservation notice if the conditions in s 107J(1) of the Act are satisfied.

	Under s 107N(1) of the Act, the AFP must give a foreign preservation notice if it receives a request in accordance with the conditions in s 107P of the Act.
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 subsection 183(2) of the *Telecommunications (Interception and Access) Act 1979*, 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 Act defines the following agencies as criminal law-enforcement agencies: • the Australian Federal Police • a Police Force of a state (as per s 5 of the Act, a state includes the Northern Territory) • the Australian Commission for Law Enforcement Integrity • the Australian Criminal Intelligence Commission • subject to subsection (1A), the Immigration and Border Protection Department (now known as the Department of Home Affairs) • the Australian Securities and Investments Commission • the Australian Competition and Consumer Commission • the NSW Crime Commission • the Independent Commission Against Corruption (NSW) • the Law Enforcement Conduct Commission • the Independent Broad-based Anti-corruption Commission • the Crime and Corruption Commission (Qld) • the Corruption and Crime Commission (WA) • the Independent Commissioner Against Corruption (SA) • subject to subsection (7), an authority or body for which a declaration under subsection (3) is in force.
Destruction of stored communications information s 150(1)	Section 150(1) of the Act sets out the circumstances under which information or records that were obtained by accessing stored communications must be destroyed. When the chief officer of an agency is satisfied that information or records are not likely to be required for a permitted purpose, they must cause the information or record to be destroyed 'forthwith'. Although the Act does not provide a definition of 'forthwith', an agency may hold itself to a particular timeframe, which will guide our assessments. Where an agency does not have a strict timeframe for destructions, in assessing compliance with this provision, our Office makes an assessment based on our

	understanding of an agency's policies and procedures and what we consider to be reasonable in the circumstances.
Disclosure by agencies to the 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 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 falls 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.
Full and free access s 186B(2)(b)	For the purpose of an inspection, the Ombudsman is entitled to have full and free access at all reasonable time to all records of the agency that are relevant to the inspection.
Historic authorisation ss 178, 178A, 179	A historic authorisation allows access to information or documents that came into existence before a carrier receives notification of the 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.
Inspection report	An inspection report presents the findings of an inspection, together with any suggestions or recommendations made in response to findings. An inspection report may be *formal* or *streamlined*. A formal report includes recommendations and is approved by the Commonwealth Ombudsman. Our Office may choose to issue a formal report where serious instances of non-compliance with the Act were identified on inspection. A draft report is provided to the agency's chief officer for comment. Agency comments are considered and, if applicable, the report is amended or updated.

	The final version of the formal report is sent to the agency's chief officer. A streamlined report outlines inspection findings and is approved by a Director of the National Assurance and Audit team. Our Office may choose to issue a streamlined report when an agency is generally compliant with the Act. The report is provided directly to an agency's line area. The agency is given the opportunity to comment on the findings. Following receipt of comments, the report is considered finalised (the streamlined report is not amended).
Journalist information warrant s 180H and s 180R-T	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 Minister. 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 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.
Interception agency s 5	The following agencies are interception agencies: • the Australian Federal Police • the Australian Commission for Law Enforcement Integrity • the Australian Criminal Intelligence Commission • an eligible authority of a state in relation to which a declaration under section 34 of the Act is in force.
Instances identified	These are issues that have been found by our Office during the course of an inspection, which are those that an agency identifies and reports to our Office.
Integrated Public Number Database (IPND or IPNDe)	The IPND is an industry-wide database which contains all listed and unlisted public telephone numbers. Information contained in the IPND may include the name and address of a customer and the type of service registered to that customer.
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 Act.
Notification to carrier s 184	When a telecommunications data authorisation or revocation is made, it is notified to the carrier. Notification may be made via: • fax • email • through Secure Electronic Disclosures Node (SEDNode), a secure electronic system used by enforcement agencies and carriers to facilitate disclosure of telecommunications data.
PJCIS	Parliamentary Joint Committee on Intelligence and Security
Pre-inspection data	Data provided by agencies to the Commonwealth Ombudsman prior to an inspection. See **Part A**.
Prescribed form s 118(1)(a)	A stored communications warrant must be in the prescribed form. The prescribed form of a stored communications warrant is set by Form 6 of Schedule 1 of the *Telecommunications (Interception and Access) Regulations 2017*.
Preservation notice s 107H, s 107N	A preservation notice is an internally issued notice which requires a carrier to preserve stored communications that relates to the person or telecommunications service specified in the notice, and hold those communications on its systems for a certain period, during which time the agency may obtain a warrant to access those communications. There are two types of preservation notices: • Domestic preservation notices • Foreign preservation notices <u>Domestic preservation notices</u> • Historic domestic preservation notice – may be given by a criminal law-enforcement agency. These notices require carriers to preserve stored communications it holds on the day the carrier receives the notice. • Ongoing domestic preservation notice – may only be given by a criminal law-enforcement agency that is an interception agency. These notices require carriers to preserve stored communications it holds at any time from when the carrier receives the notice to 29 days after receipt. <u>Foreign preservation notices</u> • If the Australian Federal Police receives a request from a foreign entity in accordance with the conditions in s 107P of the Act, the AFP must give a foreign preservation notice. These notices require carriers to preserve stored communications they hold at any time on the day the carrier receives the notice.

<table>
<tr>
<td>Privacy considerations
s 180F</td>
<td>Subsection 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 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.
</td>
</tr>
<tr>
<td>Prospective authorisation
s 180</td>
<td>A prospective authorisation enables access to information or documents that come into existence during the period for which the authorisation is in force. A prospective authorisation may also authorise the disclosure of ‘historic’ data – telecommunications data that came into existence before the time the 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 later than 45 days beginning on the day 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</td>
</tr>
</table>

	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 stored communications and 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 stored communications warrant or 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.
Receiving stored communications information s 135	Section 135(2) of the Act states the chief officer of a criminal law-enforcement agency may authorise in writing officers or classes of officers, from the agency to receive information obtained by accessing stored communications under stored communications warrants issued to the agency. For example, the chief officer may authorise certain officers by position title, or members of an investigative team, to receive stored communications accessed by a carrier under a stored communications warrant. Our Office considers stored communications information to be received for the purpose of s 135 of the Act when it is first opened and viewed.
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 the 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.

Retrospective	Our inspections of agencies' compliance with Chapters 3 and 4 of the Act operate retrospectively. This means that we are reviewing the previous financial year's records during an inspection. During our inspections conducted in the 2018–19 financial year, we reviewed records for preservation notices, warrants and authorisations that ceased to be in force in the 2017–18 financial year.
Revocation ss 107J, 107R, 122 and 180(7)	<u>Preservation notices</u> Under s 107L(2) of the Act, an agency must revoke a preservation notice if the conditions for giving a preservation notice under s 107J of the Act are no longer satisfied. A domestic preservation notice is revoked by the issuing agency giving the carrier to whom the preservation notice was given written notice of the revocation. Mandatory revocation provisions for foreign preservation notices given by the AFP are outlined under s 107R of the Act. An agency may also revoke a preservation notice at any time at its own discretion. <u>Stored communications warrants</u> Under s 122(1) of the Act, a chief officer must revoke a stored communications warrant in writing if the grounds on which the warrant was issued have ceased to exist. The written instrument of revocation must be provided 'forthwith' to the carrier to which the warrant relates. If another criminal law enforcement agency is exercising the authority of the warrant, the chief officer of the original agency must inform the chief officer of the other agency of the proposed revocation, prior to it occurring. Section 123 of the Act states that following the revocation, the chief officer of the original agency must inform the chief officer of the other agency 'forthwith' of the revocation. <u>Telecommunications data authorisations</u> Under s 180(7) of the Act, an authorised officer of a criminal law-enforcement agency must revoke the 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.
Risk mitigation	Risk mitigation in the context of our inspections is action that can be taken by agencies to reduce the likelihood of future non-compliance.
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.
Stored communication s 5	A communication that: (a) is not passing over a telecommunications system; and (b) is held on equipment that is operated by, and is in the possession of, a carrier; and (c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier. Types of stored communications: • emails • text messages (SMS) • multimedia messages (MMS) • voicemail messages.
Stored communications warrant ss 116-117	A stored communications warrant is issued under Chapter 3 of the Act. The warrant is issued in respect of a person, and instructs carriers to release preserved stored communications: • that were made by the person in respect of whom the warrant was issued; or • that another person made and for which the intended recipient is the person in respect of whom the warrant was issued; and that become, or became a stored communication before the warrant is first executed in relation to the carrier that holds the communication.
Stored communications warrants issued in	An issuing authority may issue a stored communications warrant in relation to a person who is the victim of a serious contravention if satisfied that the person is unable to consent, or it is impracticable

relation to a victim of a serious contravention s 116(1)(da)	for the person to consent, to those stored communications being accessed.
Subscriber s 5	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. Suggestions may include, but are not limited to: • updating standard operating policies and procedures • seeking legal advice • running training sessions for officers involved in using stored communications or telecommunications data powers • reviewing workplace practices to reduce the risk of non-compliance. 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.
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 Act.
Use, communication and recording s 151(1)(h)	Under Chapter 3 of the Act, agencies must keep documents or other materials that indicate whether communicating, using or recording lawfully accessed information complied with the prescribed requirements of the 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 **<u>not</u>** permitted under the Act. There are no provisions under the 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 A: Commonwealth Ombudsman stored communications inspection criteria

Audit Objective: To determine the extent of compliance with Chapter 3 of the *Telecommunications (Interception and Access) Act 1979* by the agency and its officers
1. Is the agency only dealing with lawfully accessed stored communications?
1.1 Were stored communications properly applied for?
Process checks: – Does the agency have procedures in place to ensure that warrants are in the prescribed form? **Records checks in the following areas:** – Whether applications (including telephone applications) for stored communications warrants were made in accordance with ss 111 to 114 of the TIA Act – Whether the warrant was only in relation to one person (s 117) – If the application relates to the same telecommunications service as a previous warrant – whether the application was made in in accordance with s 119(5) of the TIA Act – Whether a connection can be established between the person listed on the warrant and the relevant telecommunications service (s 117)
1.2 Was the authority of the warrant properly exercised?
Process checks: – Does the agency have procedures and authorisations in place to ensure the authority of the warrant is properly exercised? **Records checks in the following areas:** – Whether the authority of the warrant was exercised in accordance with s 127 of the TIA Act
1.3 Did the agency appropriately deal with accessed stored communications?
Process checks: – Did the agency have procedures in place to monitor and quarantine accessed stored communications? **Records checks in the following areas:** – Whether stored communications provided by the carrier were within the parameters of the warrant – Whether warrant conditions and restrictions had been adhered to – Did the agency identify stored communications that did not appear to have been lawfully accessed? – Did the agency quarantine stored communications that did not appear to have been lawfully accessed?

2. Has the agency properly managed accessed stored communications?

2.1 Were stored communications properly received by the agency?

Process checks:

- Does the agency have procedures and authorisations in place to properly receive accessed stored communications in the first instance?
- Does the agency have secure storage (whether physical or electronic) for accessed information?

Records checks in the following areas:

- Whether stored communications were received in accordance with s 135 of the TIA Act

2.2 Were stored communications properly dealt with and destroyed?

Process checks:

- Does the agency have procedures in place for the destruction of stored communications, and are they sufficient?
  Does the agency have controls, guidance and/or training in place around dealing with stored communications?

Records checks in the following areas:

- Whether any use, communication or recording of lawfully accessed information has been accounted for in accordance with ss 139 – 146 of the TIA Act
- Whether accessed stored communications were destroyed in accordance with s 150 of the TIA Act

3. Has the agency properly applied the preservation notice provisions?

3.1 Did the agency properly apply for and give preservation notices?

Process checks:

- Did the agency have procedures in place for applying for and giving preservation notices, and are they sufficient?

Records checks in the following areas:

- Whether the agency was authorised to give the preservation notice (s 107J)
- Whether the preservation notice only requested preservation for a period permitted by
  s 107H(1)(b) of the TIA Act
- Whether the preservation notice only related to one person and/or one or more services
  (s 107H(3))
- Whether the preservation notice was only issued after the relevant conditions had been met
- Whether the preservation notice was given by an authorised officer (s 107M)

3.2 Did the agency revoke preservation notices when required?

Process checks:

- Did the agency have procedures in place for revoking preservation notices and are they sufficient?

Records checks in the following areas:

- Whether the preservation notice was revoked in the relevant circumstances (s 107L)

4. Has the agency satisfied certain record keeping obligations?

Process checks:

- Did the agency have processes in place which enabled it to accurately report to the Minister on the number of preservations notices given and warrants issued (s 159)?
- Did the agency have effective record-keeping practices in place?

Records checks in the following areas:

- Whether the agency has kept records in accordance with s 151 of the TIA Act

5. Was the agency cooperative and frank?

- Is there a culture of compliance?
- Was the agency proactive in identifying compliance issues?
- Did the agency self-disclose issues?
- Were issues identified at previous inspections addressed?
- Has the agency engaged with the Commonwealth Ombudsman's office, as necessary?

Appendix B: Commonwealth Ombudsman telecommunications data inspection criteria

Audit Objective: To determine the extent of compliance with Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* by the agency and its officers
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: – Does the agency have effective procedures in place to ensure that authorisations are properly applied for, and are they sufficient? – Does the agency have effective controls, guidance and/or training in place for Authorised Officers to ensure that authorisations are properly given? – Does the agency have effective procedures in place to revoke prospective authorisations when required and notify carriers of any revocations? **Record checks in the following areas:** – Whether authorisations complied with the form and content requirements as determined by the Communications Access Coordinator (s 183(1)(f)) – Whether authorisations were made by officers authorised under s 5AB – Whether authorisations were made in relation to specified information or documents (ss 178 to 180) – Whether Authorised Officers have considered privacy in accordance with s 180F <u>*Specific to prospective authorisations*</u> – Whether prospective authorisations are in force only for a period permitted by s 180(6) – Whether prospective authorisations were revoked in relevant circumstances (s 180(7))
1.2 Did the agency identify any telecommunications data that was not within the parameters of the authorisation?
Process checks: – Does the agency have effective procedures in place to screen and quarantine telecommunications data obtained? **Record checks in the following areas:** – Whether telecommunications data obtained by the agency was within the parameters of the authorisation – Whether the agency identified any telecommunications data (including content) that did not appear to have been lawfully disclosed, and if appropriate, sought clarification from the carrier and quarantined the data from use

2. Has the agency properly managed telecommunications data?

Process checks:

- Does the agency have secure storage facilities for telecommunications data and associated information?
- Does the agency have processes in place to account for the use and disclosure of telecommunications data?

Record checks in the following areas:

- **Spot Check:** Whether the use and disclosure of telecommunications data can be accounted for in accordance with s186A(1)(g)

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

3.1 Did the agency properly apply for journalist information warrants?

Process checks:

- 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)?
- Does the agency have effective procedures in place to ensure that journalist information warrants are properly applied for and issued in the prescribed form?

Record checks in the following areas:

- Whether the application was made to a Part 4-1 issuing authority (s 180Q(1))
- Whether the application related to a particular person (s 180Q(1))
- Whether the application was made by a person listed under s 180Q(2)
- Whether the warrant was applied for a period permitted by s 180U(3), noting that no warrant extensions are permitted (s 180U(4))
- Whether the warrant was in the prescribed form and signed by the issuing authority
  (s 180U(1))

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

Records checks in the following areas:

- Whether the Ombudsman was given a copy of each warrant issued to the agency as soon as practicable (s 185D(5))
- 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))

3.3 Did the agency revoke journalist information warrants when required?

Process checks:

- Does the agency have effective procedures in place to review the continuous need for a journalist information warrant?

Record checks in the following areas:

- Whether the warrant was revoked in the relevant circumstances (s 180W)
- Whether the revocation was in writing and signed by the chief officer or their delegate
  (s 180W)