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 2019 to 30 June 2020
covering records from 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 2019 to 30 June 2020
covering records from 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 conducted by the Office of the Commonwealth Ombudsman (the Office) under s 186B of the *Telecommunications (Interception and Access) Act 1979* (the Act) from 1 July 2019 to 30 June 2020. These inspections examined agencies' records relating to stored communications and telecommunications data for the period 1 July 2018 to 30 June 2019.[1] Where we did not inspect agencies during 2018–19, our 2019–20 inspections also covered records for the period 1 July 2017 to 30 June 2018.

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 2019–20, we conducted 18 inspections of agencies' use of stored communications powers under Chapter 3 of the Act and 18 inspections of agencies' use of telecommunications data powers under Chapter 4 of the Act. Due to travel and workplace health and safety restrictions associated with COVID-19, we were unable to complete 4 inspections during 2019–20. Records from the 4 missed inspections will be inspected in 2020–21.

We made 21 recommendations in relation to 3 agencies, the Department of Home Affairs, New South Wales Police Force and Tasmania Police. We also made 237 suggestions and 77 better practice suggestions to the agencies inspected. A recommendation reflects a serious compliance issue or an issue on which an agency has not made sufficient progress. A suggestion reflects less serious and/or isolated issues where we consider an agency should take action to improve. Better practice suggestions highlight ways an agency might refine its practices where an existing practice may expose the agency to a risk of non-compliance.

Key issues identified during 2019–20 inspections include:

- Stored communications: insufficient or inconsistent data vetting and quarantining processes, non-compliance with requirements regarding destructions, historic domestic preservation notices given in a successive manner, and use and communication of stored communications.
- Telecommunications data: insufficient or inconsistent data vetting and quality control frameworks, journalist information warrant controls, sufficient seniority of authorised officers, authorised officers demonstrating consideration of the matters required under the legislation, and sufficiency of training and guidance.

For many agencies we saw an increase in the number of compliance-related findings compared to our previous inspections. While the number of recommendations made by our Office in 2019–20 decreased from 2018–19, for most agencies there was an increase in the number of suggestions and better practice suggestions since our last inspection at that agency. The results of these inspections partly reflect our Office's increased emphasis on agencies' policies, procedures, and controls in place to mitigate the risk of non-compliance. There were some instances where we were not satisfied with the remedial action taken by an agency following previous findings. In such instances, we made further suggestions or recommendations to agencies to prevent reoccurrence of the issue.

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

During our 2019–20 inspections, several of our findings stemmed from issues that were proactively identified and disclosed by agencies. Most agencies were receptive to our findings, recommendations and suggestions, indicating a strong culture of compliance.

Part A – Introduction

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

Stored communications are communications that already exist and are stored on a carrier's systems and 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 a 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 several 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. The individual will not know access has occurred and will not be able to use complaint or other review mechanisms that would ordinarily be available if an individual considers action has been taken unreasonably. Independent oversight of these powers is essential, particularly for telecommunications data because the decision to authorise an 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 justification and proportionality of the privacy intrusion. If agencies cannot demonstrate they are acting consistently with their legislative obligations, we cannot assure Parliament and the public 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.

We provide an agency with our preliminary inspection findings verbally at an exit interview and invite its staff to provide any initial comments. We then provide an agency with a written report containing the results of our inspection and our assessment of its legislative 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 Parliament.

This report is divided into 5 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 2019–20 inspection period.

- Part B highlights the importance of a culture of compliance.
- Parts C and D set out the results of our stored communications and telecommunications data inspections respectively.
- Appendices A and B set out our stored communications and telecommunications data inspection criteria.
- Appendix C provides a glossary of key terms used throughout the report.

Agencies we oversee

Currently, 20 agencies can use the stored communications and telecommunications data powers under the Act (see the table in Appendix C). The Minister may declare additional agencies in prescribed circumstances but did not make any such declarations in 2018–19.[2] We do not oversee telecommunication service carriers.

Inspections conducted in 2019–20

In 2019–20, our Office conducted 18 inspections of agencies' use of stored communications powers under Chapter 3 of the Act and 18 inspections of agencies' use of telecommunications data powers under Chapter 4 of the Act. The agencies inspected are set out in Parts C and Part D.

The Act does not specify the frequency of these inspections. Our Office scheduled inspections for all 20 agencies who can use stored communications and telecommunications data powers during 2019 –20. Due to travel restrictions associated with COVID-19 we were unable to complete inspections for the following agencies:

- stored communications under Chapter 3 of the Act: LECC and Victoria Police
- telecommunications data under Chapter 4 of the Act: LECC and IBAC.

These agencies will be inspected by our Office in 2020–21.

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 considering the 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 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 helps agencies to achieve compliance by assessing policies and procedures, communicating better practices, facilitating communication across agencies and engaging with agencies outside of inspections.

[2] Our inspections in 2019—20 considered use of the powers during 2018—19.

Stakeholder engagement

During 2019–20, 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 presentations at agency induction and training sessions for staff and compliance advice provided to agencies via email. This engagement outside of inspections assists our Office to obtain a greater understanding of the issues faced by agencies when applying these powers. It also enables the Office to bring to agencies' attention risks to non-compliance identified through our oversight function.

Part B – Culture of compliance

During our inspections of an agency's use of powers under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979* (the Act), we assess compliance with the Act against our inspection criteria to determine if an agency has a strong culture of compliance. We look at whether an agency:

- was proactive in identifying compliance issues including disclosing issues
- adequately addressed issues identified at previous inspections
- provides training, guidance and support to officers exercising the powers
- engaged with our Office and was cooperative and frank.

We consider that a strong culture of compliance promotes 'compliance self-sufficiency,' where agencies can confidently navigate the legislative framework and establish necessary processes to achieve compliance.

Agencies with a strong culture of compliance provide effective training and support to staff exercising covert 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 culture of compliance 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.

It is important that agencies proactively assess their own records at the time the records are made 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 an agency continuing to make the same errors, before we identify the issue at our inspection.

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

In addition to the recommendations, suggestions and better practice suggestions we made to agencies in relation to telecommunications data and stored communications findings (see Parts C and D), we made 4 recommendations to Tasmania Police regarding its overall approach to compliance as set out in case study 1.

The 2 case studies below illustrate this approach and the impact an agency's culture of compliance can have on its ability to implement improved compliance mechanisms. Specifically, case study 1 shows the broader effects the lack of a culture of compliance has on an agency's ability to identify and reflect on compliance issues. Case study 2 illustrates that responsiveness and proactive action 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 2019–20. 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 and not just the agencies about which the case study is written.

Case Study 1 – Tasmania Police

During our 2018–19 inspection we identified that Tasmania Police did not have a well-developed culture of compliance and made recommendations in relation to Tasmania Police's compliance mechanism and culture.

Developing compliance mechanisms and a culture of compliance is an ongoing process. However, following our 2019–20 inspection we were not satisfied that Tasmania Police had taken sufficient action to address our previous recommendations and remained of the view that Tasmania Police needed to implement further compliance-focused guidance material and training for exercising the powers under Chapters 3 and 4 of the Act.

While Tasmania Police had taken positive steps to establish awareness amongst staff of their legislative obligations, we were of the view there remained a need for further work to address this issue. We found a lack of detailed or authoritative agency-level policies and procedures to assist officers in their decision making about the application of telecommunications data or stored communications powers, or to support officers to confidently navigate and understand the legislative framework.

Tasmania Police is yet to implement a compliance-focused approach to using these intrusive powers. We made the following recommendations to Tasmania Police:

- **Recommendation 1:** Tasmania Police should implement regular and comprehensive training to ensure all staff involved in using the powers in Chapters 3 and 4 of the Act have and maintain a thorough understanding of the legislative framework and their responsibilities.

- **Recommendation 2:** Tasmania Police should develop compliance driven guidance for all staff involved in using the powers in Chapters 3 and 4 of the Act. This guidance should be easily accessible to staff and provide clear advice about how to address each of the specific legislative requirements so staff can confidently navigate these provisions to achieve compliance.

- **Recommendation 3:** Tasmania Police should develop a compliance program to foster a compliance-focused approach to using the powers under Chapters 3 and 4 of the Act with a view to improving transparency, accountability, responsiveness, and self-evaluation.

During our 2019–20 inspection Tasmania Police was not able to clearly identify or demonstrate the remedial action it had taken to address our previous findings.

As such, we also made the following recommendation:

- **Recommendation 4:** Tasmania Police should revise its inspection preparation practices to ensure it is able to engage with and respond to previous inspection findings, including demonstrating it has considered and taken action to address issues identified in inspections and disclosing any instances of non-compliance to our Office.

In response to these recommendations, Tasmania Police advised our Office that it is committed to developing a strong compliance culture and outlined steps it is taking to provide comprehensive training and guidance to staff. We will assess action taken by Tasmania Police at our next inspection.

Case Study 2 – Independent Broad-based Anti-corruption Commission

During our 2019–20 inspection the IBAC disclosed instances where preservation notices were given under Chapter 3 of the Act in contravention of a condition for giving such notices under s 107J(1)(e) of the Act.

Prior to our inspection the IBAC self-identified the issue, determined the likely cause and took steps to prevent reoccurrence (discussed further at Part C of this report). While we suggested the IBAC take further remedial action, the IBAC's transparency to our Office and proactive action is indicative of the IBAC'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 Telecommunications (Interception and Access) Act 1979 (the Act) the Ombudsman must inspect records of a criminal law-enforcement agency to determine the extent of compliance by that agency and its officers 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 already exist, are stored in a carrier's systems and contain the content of the communication. Examples of stored communications include Short Message Service (SMS), Multimedia Messaging Service (MMS), emails and voicemails.

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 3 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 give preservation notices but will assess agencies' compliance in giving such notices against the requirements of Chapter 3 of the Act.

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 2019–20 is set out at Appendix A.

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

Summary of stored communications findings

During 2019–20 our Office inspected 18 agencies' access to stored communications under Chapter 3 of the Act. In most instances our inspections covered records for the period 1 July 2018 to 30 June 2019. Where we did not inspect agencies during 2018–19, we also inspected the agency's records for the period 1 July 2017 to 30 June 2018 during our 2019-20 inspections.

Often, though not in all cases, we made a greater number of compliance related findings at agencies with higher usage of the stored communications powers. We also note that several agencies had not been inspected by our Office for several years. We did not inspect some agencies in 2018–19 because of a risk-based assessment taken by our Office for that inspection year. There were 3 agencies[4] where it had been 2 to 3 years since our last stored communications inspection.

Several of our findings related to issues that agencies proactively identified and disclosed.

While we were satisfied with the remedial action taken by many agencies in response to our previous inspection findings, there were several agencies where issues reoccurred or where we were not satisfied with the remedial action taken. In such instances, we made further suggestions or recommendations to agencies including regarding improving processes to prevent reoccurrence of the issue.

Agencies not inspected in relation to Chapter 3 of the Act during 2019–20

Due to COVID-19 restrictions, our Office was required to temporarily pause inspections in mid-March 2020. As a result, we did not inspect all agencies' compliance with Chapter 3 of the Act. We did not inspect the LECC or Victoria Police. We will inspect a sample of these 2 agencies' records that were unable to be completed at our 2020–21 inspections.

Recommendations and suggestions made during 2019–20

A recommendation reflects a serious compliance issue or a previously identified issue on which an agency has not made sufficient progress. A suggestion reflects less serious and/or isolated issues where we consider an agency should take action to improve. Better practice suggestions highlight ways an agency might refine its practices where existing practice may expose the agency to a risk of non-compliance.

[4] The ACCC, ACLEI and ASIC.

Table 1 – Number of recommendations, suggestions, better practice suggestions made per agency during the 2019–20 inspection period from stored communications inspections

Agency	Recommendations	Suggestions	Better practice suggestions
ACCC	-	4	2
ACIC	-	1	2
ACLEI	-	1	1
AFP	-	12	4
ASIC	-	3	2
CCC QLD	-	7	2
CCC WA	-	-	-
Home Affairs	-	5	2
IBAC	-	1	1
ICAC NSW	-	8	1
ICAC SA	-	3	1
LECC	Not inspected		
NSW CC	-	-	2
NSW Police	-	8	3
NT Police	-	6	-
QPS	-	3	3
SA Police	-	1	1
Tasmania Police	2	9	1
Victoria Police	Not inspected		
WA Police	-	1	1
TOTAL:	**2**	**73**	**29**

Table 2 – Use of stored communications powers and records inspected in the 2019-20 period [5]

Agency	Records period inspected	Total Historic PN[6]	Historic Inspected	Total Ongoing PN	Ongoing inspected	Stored Comms Warrants	Warrants inspected	Total inspected
ACCC	17–18, 18–19	12	**9**	-	**-**	9	**9**	**18**
ACIC	18–19	2	**2**	5	**5**	2	**2**	**9**
ACLEI	17–18, 18–19		**-**	3	**3**	4	**4**	**7**
AFP	18–19	103	**22**	79	**17**	94	**39**	**78**
ASIC	17–18, 18–19	94	**94**	-	**-**	2	**2**	**96**
CCC QLD	18–19	-	**-**	22	**15**	3	**3**	**18**
CCC WA	17–18, 18–19	1	**1**	2	**1**	1	**1**	**3**
Home Affairs	18–19	10	**10**	-	**-**	9	**9**	**19**
IBAC	17–18, 18–19	1	**1**	17	**8**	4	**4**	**13**
ICAC NSW	17–18, 18–19	7	**6**	7	**6**	7	**7**	**19**
ICAC SA	18–19	-	**-**	11	**11**	-	**-**	**11**
NSW CC	17–18, 18–19	-	**-**	7	**7**	6	**6**	**13**
NSW Police	18–19	817	**47**	92	**10**	705	**58**	**115**
NT Police	17–18, 18–19	60	**7**	24	**1**	6	**6**	**14**
QPS	18–19	19	**9**	220	**41**	165	**45**	**95**
SA Police	17–18, 18–19	161	**26**	47	**7**	43	**32**	**65**
Tasmania Police	18–19	15	**2**	127	**16**	50	**14**	**32**
WA Police	18–19	74	**14**	71	**15**	48	**20**	**49**
TOTAL:		**1,376**	**250**	**734**	**163**	**1,158**	**261**	**674**

Compliance issues and risks to compliance

This section outlines instances of non-compliance we identified across multiple agencies during our 2019–20 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 the 2019–20 reports at future inspections.

Data vetting and quarantining processes

Under s 117 of the Act, a stored communications warrant authorises an approved person to access stored communications made or intended to be received by the person named on the warrant subject to any conditions or restrictions specified on the warrant. Any stored communications received outside the parameters of the relevant stored communications warrant should be quarantined from use or communication. It is important that an agency has processes that enable it

[5] Does not include foreign preservation notices issued by the Australian Federal Police.

[6] Preservation notices (PNs).

to consistently vet data received, identify any stored communications that have been unlawfully obtained and effectively quarantine any such data.

In assessing data vetting and quarantining processes, our Office also looks for records demonstrating action taken to quarantine any unlawfully accessed information and confirmation the information was not used, communicated, or recorded.

During our 2019–20 inspections we identified instances where agencies were undertaking data vetting but did not have an established policy guiding this process and did not keep records of checks completed. We also identified instances where we were not satisfied that agencies were able to consistently identify and manage unlawfully accessed stored communications.

We made recommendations and suggestions to 5 of 18 agencies regarding the need to have established procedures and mechanisms for data vetting and quarantining stored communications received outside the parameters of the relevant warrant.

One of the most significant findings we made about data vetting processes involved instances where stored communications warrants had ceased to be in force at the time the carrier accessed the stored communications. Under s 119(1) of the Act a stored communications warrant remains in force until it is first executed or until the end of 5 days after the day it was issued, whichever occurs sooner. A warrant is executed at the time a carrier first accesses the relevant stored communications under the warrant. To determine whether a carrier has accessed stored communications while the relevant warrant is in force, agencies provide the carrier with a blank *'Response to a stored communications warrant issued under the Telecommunications (Interception and Access) Act 1979'* coversheet. The carrier will then complete and return the coversheet to the agency noting the date and time it accessed the stored communications.

At 4 of the 18 agencies we inspected in 2019–20 there were instances where the agency received stored communications that were accessed by a carrier after the relevant warrant had ceased to be in force. In such circumstances we consider the stored communications were not lawfully accessed, and the stored communications should be quarantined and not used, communicated, or recorded by the agency.

In some agencies this was identified at the time of receipt of the stored communications and appropriate remedial action was taken. In other instances where the agency did not identify and quarantine the affected stored communications, we made suggestions regarding improving data vetting processes to manage such instances. In these instances, the agency advised our Office the unlawfully accessed stored communications were quarantined.

Destruction of stored communications

Where the chief officer of an agency is satisfied that information or a record obtained by accessing a stored communication is not required for a permitted purpose, the information or record must be destroyed 'forthwith'. Chapter 3 of the Act requires destruction of both the original stored communications information and records, and any copies created, to be done in accordance with s 150(1) of the Act. No stored communications should be destroyed without appropriate written approval under s 150(1) of the Act.

As 'forthwith' is not defined in the Act an agency may set a particular timeframe for itself. In conducting our compliance assessments we will be guided by the agency's internal timeframe but will also consider whether this timeframe is a reasonable period of time in the circumstances noting the ordinary definition of 'forthwith' as immediate and without delay.

Achieving compliance with destruction requirements requires agencies to have a strong framework in place to track all relevant stored communications, seek appropriate approval from the chief officer under s 150(1) of the Act and ensure destruction of relevant records and information (including copies) forthwith. Robust record-keeping and document tracking processes reduce delays in accounting for records after the chief officer has certified records for destruction. It is also important that agencies have clear guidance available to staff regarding the destruction requirements to achieve compliance with s 150(1) of the Act.

We made findings in relation to destructions of stored communications at 10 of the 18 agencies inspected during 2019–20. Issues identified included:

- destruction of stored communications that did not take place 'forthwith'
- inadequate record keeping resulting in our Office being unable to determine if stored communications had been destroyed and, in some instances, whether destruction occurred before or after chief officer approval
- agency processes that require an investigator (rather than the chief officer) to decide whether the stored communications are not required for a permitted purpose
- stored communications that were certified for destruction by the chief officer but were not destroyed at the time of our inspection.

We continue to identify destruction related issues across many agencies when assessing compliance with Chapter 3 of the Act. This will be an area of focus for our Office in conducting our 2020–21 inspections and we strongly encourage agencies to take action to remediate their processes.

Historic domestic preservation notices given in a successive manner

There are 2 types of domestic preservation notices under Chapter 3 of the Act:

- a historic domestic preservation notice requires a carrier to preserve the relevant stored communications it holds at any time on or before the day it received the notice
- an ongoing domestic preservation notice requires a carrier to preserve the communications it holds from the time it receives the notice until 29 days after the day it receives the notice.

Only a criminal law-enforcement agency that is an 'interception agency', as defined by the Act, may give an ongoing domestic preservation notice.

During 2019–20, we again identified a practice where an agency that is not an interception agency gave historic domestic preservation notices in a successive manner about the same person or telecommunications service to the same carrier. This practice results in a carrier preserving stored communications over several days rather than on the day a (single) notice was received which is the intended operation of a historic domestic preservation notice as per s 107H(1)(b)(i) of the Act.

There is no express legislative provision that prohibits this practice. However, in our view it circumvents the intended operation of the Act for a non-interception agency to give historic domestic preservation notices in a successive manner simulating the effect of an ongoing domestic preservation notice (which those agencies are not authorised to give).

There may be circumstances where an agency has legitimate cause to issue more than one historic domestic preservation notice about the same person or telecommunications service. This can be distinguished from instances where historic domestic preservation notices are issued successively on the same basis giving the effect of an ongoing domestic preservation notice.

Compliance is assessed on a case by case basis and our Office may make a finding that successive historic domestic preservation notices are given in a manner contrary to the intended operation of the Act in circumstances including where:

- Successive historic domestic preservation notices are given as a matter of course for the purpose of capturing stored communications across a period beyond what the carrier would preserve under one historic domestic preservation notice.
- Historic domestic preservation notices are issued successively on the same basis without a change of circumstances.

Following our 2019–20 inspections our Office provided further guidance to non-interception agencies about this matter and our approach to assessing compliance during inspections. This guidance was prepared in consultation with the Department of Home Affairs as the administrator of the Act.

Using, communicating, and recording stored communications

In conducting our compliance inspections, we look at whether an agency has processes in place to meet its record-keeping obligations regarding using, communicating, and recording stored communications under Chapter 3 of the Act.

It is important that agencies have a consistent process for documenting any use, communication and recording of stored communications to:

- accurately account for whether stored communications were used, communicated, or recorded for a permitted purpose under Chapter 3 of the Act
- demonstrate that quarantining of any unlawfully accessed information has occurred and confirm that information has not been used, communicated, or recorded in instances where stored communications were received outside the parameters of a valid warrant
- track copies of stored communications and records to fulfil destruction requirements
- ensure it can satisfy its record-keeping obligations under s 151(1)(h) of the Act.

We made findings about keeping records of using, communicating, or recording stored communications at 4 of the 18 agencies inspected in 2019–20. We made suggestions to agencies to establish a consistent process for keeping records to accurately account for whether stored communications were used, communicated or recorded for a permitted purpose to ensure agencies satisfy their record keeping obligations under s 151(1)(h) of the Act.

Prescribed form of stored communications warrants

Section 118(1)(a) of the Act requires a stored communications warrant to be in the prescribed form, set by Form 6 of Schedule 1 of the *Telecommunications (Interception and Access) Regulations 2017* (the Regulations). During 2019–20, we made findings regarding the prescribed form of stored communications at 11 of the 18 agencies inspected.

We identified instances where agencies had deleted non-applicable paragraphs from their warrants including deleting the conditions and restrictions paragraphs of the prescribed form. This is consistent with direction given in Form 6, which states agencies can “Omit if not applicable” certain paragraphs of the warrant. However, as a matter of better practice our Office suggests agencies strike through (rather than delete) the fields the Regulations stipulate can be omitted if not applicable. This practice:

- ensures that officers consider the potential relevance of each field when preparing a warrant
- enables an issuing authority to turn their mind to the relevant considerations
- mitigates the risk that a warrant may inadvertently not include one of the mandatory fields by keeping the paragraph numbers consistent with Form 6.

- is consistent with advice provided to agencies by the Office of the Communications Access Coordinator in the Department of Home Affairs.

At 11 of the 18 agencies inspected we also noted instances where stored communication warrants or warrant templates did not strictly comply with the prescribed form due to additional text being included or issues with paragraph numbering.

We identified instances where warrants were issued for services associated with a particular person. Under s 110(1) of the Act a criminal law-enforcement agency may apply to an issuing authority for a stored communications warrant for a person. As per the prescribed form, a stored communications warrant is to state the name of the person including other identifying information. Where an agency also wishes to specify the service number on the warrant to restrict access to only the stored communications of that particular service number, this could be entered as a restriction on the warrant under paragraph 5 of the prescribed form. This approach ensures it is clear a warrant is issued in respect of a person (rather than a service number) as required by the Act, and that the service number is not merely an identifying particular but a limit on the scope of the warrant sought.

Findings from stored communications inspections conducted in 2019–20

Below we summarise the main findings for the 18 agencies we inspected during 2019–20.

After receiving our inspection report agencies often tell us about remedial action 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 Commission for Law Enforcement Integrity

We inspected ACLEI from 16 to 18 September 2019 covering records of ACLEI's use of stored communications powers for the period 1 July 2017 to 30 June 2019. We made **one suggestion** and **one better practice suggestion** and sent ACLEI a report outlining our findings on 21 February 2020.

Table 3 – Stored communications inspection statistics: Australian Commission for Law Enforcement Integrity

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Ongoing domestic preservation notices	3	3 (100%)
Stored communications warrants	4	4 (100%)

Progress since previous inspection

We made one suggestion to ACLEI at our previous inspection conducted in 2015–16, regarding non-compliance with a condition for an ongoing domestic preservation notice. This issue was not identified during this inspection.

Significant findings

Using, communicating, and recording stored communications

During the inspection ACLEI was unable to locate records to confirm how the stored communications obtained under the 4 warrants were used or communicated. We suggested ACLEI seek to determine how the stored communications were used and communicated and make records detailing any use and communication in line with s 151(1)(h) of the Act. In its response, ACLEI advised of procedural changes to improve record-keeping.

Prescribed form of stored communications warrants
We identified the 4 stored communications warrants issued to ACLEI that deleted the items in the prescribed form that allow the authority to specify any conditions or restrictions that the warrant is subject to. As a matter of better practice, we suggested that ACLEI include these fields on the warrant even if ACLEI is not proposing the warrant be subject to conditions or restrictions, to enable an issuing authority to turn their mind to this issue. ACLEI advised that it will follow this practice in the future.

Table 4: Inspection findings: Australian Commission for Law Enforcement Integrity

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Were stored communications properly applied for?				
Prescribed form of stored communications warrants	4	-	1 better practice suggestion	s 118(1)(a) Form 6[7]
Has the agency satisfied certain record keeping obligations?				
Compliance with record keeping obligations regarding use, communication, and recording	4	-	1 suggestion	s 151(1)(h)

2. Australian Competition and Consumer Commission

We inspected the ACCC from 9 to 12 December 2019 covering records of the ACCC's use of stored communications powers for the period 1 July 2017 to 30 June 2019.We made **4 suggestions** and **2 better practice suggestions** and sent the ACCC a report outlining our findings on 22 May 2020.

Table 5 – Stored communications inspection statistics: Australian Competition and Consumer Commission

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	12	9 (75%)
Stored communications warrants	9	9 (100%)
Destruction of stored communications information	9	9 (100%)

Progress since previous inspection
We made one suggestion to the ACCC at our previous inspection conducted in 2015–16 , regarding preservation notices given for more than one person which is not provided for under the Act. This issue was not identified during this inspection

Significant findings
Stored communications warrants no longer in force at the time of carrier access
The ACCC disclosed one instance to our Office where a carrier accessed stored communications when the related stored communications warrant was no longer in force. We also identified

[7] Form 6 of Schedule 1 of the *Telecommunications (Interception and Access) Regulations 2017* (the Regulations).

3 instances where, after receiving stored communications under a warrant, the ACCC obtained further hardcopies of the stored communications from the carrier after the warrant ceased to be in force. In all instances the stored communications were not used or communicated by the ACCC and were destroyed.

We suggested the ACCC review internal guidance and training materials to ensure staff exercising these powers understand when a warrant ceases to be in force and are able to identify instances where stored communications are accessed by a carrier after the warrant has ceased. The ACCC advised it would clarify internal guidance to clearly outline when a warrant ceases to be in force.

Prescribed form of stored communications warrants

We identified that the ACCC's warrant template did not include paragraph 2(e) of the prescribed form which relates to victims of serious contraventions. The Act requires stored communications warrants to be in the 'prescribed form' found in Form 6 of the Regulations. We suggested the ACCC update its stored communications warrant template to align with the prescribed form. Including this paragraph in the ACCC's warrant template ensures officers consider the potential relevance of s 116(1)(da) of the Act (which relates to stored communications warrants applied for in relation to victims) when preparing a warrant. In addition, it mitigates the risk that a warrant may inadvertently not include one of the mandatory fields by keeping the paragraph numbers consistent.

We also identified 5 warrants deleted the items in the prescribed form that enable the issuing authority to specify any conditions or restrictions that the warrant is subject to. We made a better practice suggestion for the ACCC to strike out non-applicable paragraphs or state nil for the conditions and restrictions paragraphs rather than deleting them, to enable an issuing authority to turn their mind to this issue. The ACCC advised it had updated its warrant template to comply with the prescribed form and will add guidance in relation to striking through non-applicable paragraphs.

Destruction of stored communications

We identified that not all stored communications were destroyed forthwith in accordance with the requirements under s 150(1) of the Act. In one instance a copy of the stored communications was still held by the ACCC. The ACCC organised for the stored communications to be subsequently destroyed. We will confirm the destruction of this record at our next inspection.

Table 6 – Inspection findings: Australian Competition and Consumer Commission

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Stored communications warrant accessed by carrier after warrant ceased to be in force	3	1	1 suggestion	s 119(1)
Prescribed form of stored communications warrants	General finding 5	-	1 suggestion 1 better practice suggestion	s 118(1)(a) Form 6
Unable to determine who exercised the authority of a warrant	3	-	1 better practice suggestion	s 127(1) s 127(2)
Has the agency properly managed accessed stored communications?				
Stored communications not destroyed forthwith	1	-	-	s 150(1)
Destruction not reported to the Minister	1	-	1 suggestion	s 150(2)

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Other findings				
Unable to assess stored communications received due to destruction	General finding		1 suggestion	s 117 s 150(1)

3. Australian Criminal Intelligence Commission

We inspected the ACIC from 29 July to 2 August 2019 covering records for the period 1 July 2018 to 30 June 2019. We made **one suggestion** and **2 better practice suggestions** and sent the ACIC a report outlining our findings on 8 January 2020.

Table 7 – Stored communications inspection statistics: Australian Criminal Intelligence Commission

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	2	2 (100%)
Ongoing domestic preservation notices	5	5 (100%)
Stored communications warrants	2	2 (100%)

Progress since previous inspection

We made one suggestion to the ACIC at our previous inspection conducted in 2018–19, regarding non-compliance with a condition for an ongoing domestic preservation notice. This issue was identified again during this inspection. We made a further suggestion to the ACIC as discussed below.

Significant findings

Conditions for giving preservation notices

At this inspection we identified one preservation notice that was given after the relevant warrant had been issued. This created ambiguity about the validity of the preservation notice as the condition under s 107J(1)(d) of the Act was not met. While this may have been a historic issue, we suggested the ACIC seek advice as to whether the conditions for giving a preservation notice are met if an agency is considering giving a preservation notice where a relevant warrant has already been issued. The ACIC advised that it was creating a preservation notice checklist to record, centralise and improve quality assurance activities and had updated preservation notice content within relevant training and induction material and acknowledged our finding and suggestion.

Prescribed form of stored communications warrants

We identified 2 instances where stored communications warrants issued to the ACIC did not include all the wording specified in the prescribed form. In addition, we noted inconsistencies in the way the ACIC omitted non-applicable paragraphs from the warrant, with 2 warrants striking through one non-applicable paragraph and deleting a different non-applicable paragraph. As a matter of better practice, we suggested the ACIC ensure its warrant template aligns with the prescribed form and that it adopts a consistent method of omitting non-applicable paragraphs from the warrant. The ACIC advised that it would strike through non-applicable paragraphs.

Table 8 – Inspection Findings: Australian Criminal Intelligence Commission

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Prescribed form of stored communications warrants	2	-	1 better practice suggestion	s 118(1)(a) Form 6
Has the agency properly managed accessed stored communications?				
Destruction of temporary files	7	-	1 better practice suggestion	s 150(1)
Has the agency properly applied the preservation notice provisions?				
Condition for giving a preservation notice not met	1	-	1 suggestion	s 107H(2) s 107J(1)(d)
Invalid preservation notices	-	2	-	s 117
Preservation notice not revoked	-	1	-	s 107L(2)(a)

4. Australian Federal Police

We inspected the AFP from 20 to 23 January 2020 covering records for the period 1 July 2018 to 30 June 2019. We made **12 suggestions** and **4 better practice suggestions** and sent the AFP a report outlining our findings on 1 July 2020.

Table 9 – Stored communications inspection statistics: Australian Federal Police

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	103	22 (21%)
Ongoing domestic preservation notices	79	17 (22%)
Foreign preservation notices	5	5 (100%)
Stored communications warrants	94	39 (41%)
Destruction of stored communications information	34	22 (65%)

Progress since previous inspection

We made 2 recommendations and 15 suggestions (including 4 better practice suggestions) to the AFP at our inspection conducted in 2018–19. While the AFP took appropriate remedial action to address some of these issues, we again identified instances of unlawfully accessed stored communications not being identified and quarantined and stored communications not destroyed forthwith.

Significant findings

Stored communications warrant had expired at the time of carrier access

We identified one instance where stored communications were accessed by the carrier after the stored communications warrant expired. We suggested the AFP quarantine the relevant stored

communications and introduce further controls into its screening process to assist in identifying all instances where stored communications received are either outside the parameters of the warrant or were accessed by the carrier after the warrant has ceased. The AFP advised the stored communications had been quarantined and that a further control was added to check that stored communications received are within the parameters of the warrant.

Successive warrant issued in contravention of s 119(5) of the Act

We identified one instance where a stored communications warrant was invalidly issued within 3 days of a previous warrant being executed which related to the same person and telecommunication service in contravention of s 119(5) of the Act. We note the AFP sought an amendment to the original warrant to correct an administrative error, however a new warrant was issued. The AFP did not execute the second invalid warrant. We suggested the AFP provide further education to officers regarding the requirements under s 119(5) of the Act for subsequent stored communications warrants about the same telecommunications service. The AFP undertook to provide further guidance to officers.

We also identified the affidavits accompanying several warrants did not identify previous relevant warrants about the same person or telecommunication service. They included an express statement incorrectly stating there were no previous warrants or identified some but not all previous warrants. While this is not a strict legislative requirement, we consider there is a risk that a warrant may be issued contrary to s 119(5) of the Act if the issuing authority is unaware of the details regarding any previous warrants issued for the same telecommunication service. We suggested the AFP include detail in affidavits regarding whether any previous warrants were issued in relation to the same person or telecommunication service as a matter of better practice to mitigate this risk. The AFP advised that our better practice suggestion had been communicated to relevant officers.

Destruction of stored communications

We identified 3 instances where the AFP's destruction of stored communications information was not completed forthwith as required by s 150(1) of the Act, when measured against AFP's standard operating procedure. The Act does not define 'forthwith'. The AFP's standard operating procedure states destructions should be completed within 20 business days. The records we identified were not destroyed until over 2 months after the destruction was authorised. In a further 2 instances the AFP's destructions paperwork was inconsistent and we were unable to determine if or when stored communications had been destroyed. We suggested the AFP take steps to ensure it can complete its destructions process within its internal 'forthwith' timeframe. The AFP subsequently advised it would act in line with our suggestion.

Conditions for giving foreign preservation notices

We identified 2 instances where the written request to the AFP to preserve stored communications by a foreign entity did not specify that the foreign entity intended to make a mutual assistance request to access the stored communications as required under s 107P(2)(h) of the Act. We suggested the AFP ensures that requests received from foreign entities to preserve stored communications meet the conditions under s 107P of the Act for foreign preservation notices and engage further with the foreign entity where necessary. The AFP advised that further training has been provided to officers and that requests not meeting the legislative requirements would be referred back to the foreign entity to provide all required information.

Table 10 – 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 accessed by carrier after warrant ceased to be in force	1	-	2 suggestions	s 119(1)
Successive warrant issued in contravention of s 119(5) of the Act	1	-	1 suggestion	s 119(5)
Addressing whether there were previous warrants in affidavits	20	-	1 better practice suggestion	
Content of affidavits accompanying applications for stored communications warrants	-	2	1 suggestion 1 better practice suggestion	s 113 s 116(1)(d)(i) s 117 s 118(3)
Identifying the person exercising the authority of the warrant	2	-	1 better practice suggestion	s 127
Revoking stored communications warrants	5	-	1 suggestion	s 122(1) s 151(1)(d)
Legacy issue: Prescribed form for stored communications warrants	General finding	-	-	s 118(1)(a) Form 6
Has the agency properly managed accessed stored communications?				
Referencing the correct legislative provision for the receipt of stored communications	6		1 suggestion	s 135(2)
Stored communications information not destroyed forthwith or where we were unable to confirm if and when destructions occurred	5[8]	-	2 suggestions	s 150(1) s 150(2)
Destruction reports to the Minister	8	-	1 suggestion	s 150(2)
Has the agency properly applied the preservation notice provisions?				
Conditions for giving a foreign preservation notice not met	2	-	1 suggestion	s 107P

[8] 3 instances where the AFP's destructions of stored communications information were not conducted 'forthwith' and 2 instances where the AFP's destructions paperwork was inconsistent, and we were unable to determine if or when stored communications had been destroyed.

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Partial revocation of preservation notices	1	-	1 suggestion	s 107L(1) s 107K(b)(ii) s 107L(3)
Has the agency satisfied certain record keeping obligations?				
Annual report inaccuracies	5	-	1 suggestion	s 159 s 162(2)(d)
Was the agency cooperative and frank?				
Disclosure log	-	2	1 better practice suggestion	-

5. Australian Securities and Investments Commission

We inspected ASIC from 21 to 24 October 2019 covering records for the period 1 July 2017 to 30 June 2019. We made **3 suggestions** and **2 better practice suggestions** and sent ASIC a report outlining our findings on 15 April 2020.

Table 11 – Stored communications inspection statistics: Australian Securities and Investments Commission

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	94	94 (100%)
Stored communications warrants	2	2 (100%)
Destructions of stored communications information	4	4 (100%)

Progress since previous inspection

We made one suggestion to ASIC from our previous inspection conducted in 2016–17 , regarding a discrepancy in its reporting to the Minister. ASIC subsequently issued an addendum to the Minister correcting its reporting. We also commented on a practice where ASIC gave successive historic domestic preservation notices. This issue was identified again during our 2019-20 inspection.

Significant findings

Historic domestic preservation notices given in a successive manner

We identified 2 instances where ASIC gave a series of 47 consecutive historic domestic preservation notices to the same carrier in relation to the same person. There is no express legislative provision that prohibits this practice. However, in our view it bypasses the intended operation of the Act for ASIC (a non-interception agency) to give historic domestic preservation notices in a successive manner simulating the effect of an ongoing domestic preservation notice (which ASIC is not authorised to give).

We suggested that ASIC revise its policies and procedures to ensure it does not give successive historic domestic preservation notices to the same carrier where the notice specifies the same telecommunications service or person.

ASIC advised that its procedural document has been amended to require additional consultation and approval before any successive historic domestic preservation notices are issued and the issue of successive historic domestic preservation notices will be subject to approval on a case-by-case basis.

Our Office engaged further with ASIC about this matter and provided further advice regarding circumstances where our Office may find the practice of giving historic domestic preservation notices bypasses the intended operation of the Act. We will review ASIC's amended procedural document and any changes to its practice at our next inspection.

Stored communications information received by unauthorised persons

We identified 2 instances where stored communications were received by officers not authorised to do so under ASIC's s 135(2) authorisation. We consider that the officer who first opens and views the stored communications is the person receiving the information for the purposes of s 135 of the Act. We suggested that ASIC ensure any staff who receive stored communications are appropriately covered by a s 135 authorisation. We understand that ASIC acted to mitigate the reoccurrence of this issue.

Prescribed form of stored communications warrants

We identified one instance where a stored communications warrant was issued in respect of a person and 2 services. A stored communications warrant can only be issued in respect of a person. ASIC wished to identify these services as they were subscribed in the name of a person other than the person of interest listed on the warrant. We noted the form of this warrant was non-compliant with the prescribed form and s 118 of the Act. Due to our concern this may have impacted the validity of the warrant and the stored communications information obtained under the warrant we suggested that ASIC seek advice regarding the validity of the warrant. ASIC advised the investigation involving this warrant was discontinued without further action and all stored communications obtained under the warrant were destroyed.

ASIC advised that it intends to amend its procedural document and precedents in accordance with our advice regarding entering service numbers under the restrictions paragraph of warrants. We consider this to be appropriate remedial action to mitigate the risk of this issue occurring in future warrants. We will review amendments to ASIC's procedural document and stored communications warrant precedents at our next inspection.

Destruction of stored communications

ASIC disclosed a delay in the certification of stored communications for destruction under s 150(1) of the Act. The stored communications were subsequently destroyed once identified by ASIC. ASIC advised of improvements to be made to its destructions process and reminded investigators of the destruction obligations. ASIC also advised of updates to its procedural document. We will review the procedures that ASIC has in place for identifying and destroying stored communications that are no longer required for a permitted purpose at our next inspection.

Table 12 – Inspection findings: Australian Securities and Investments Commission

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Prescribed form of warrants	1	-	1 suggestion	s 110(1) s 117 s 118(1)(a) Form 6
Has the agency properly managed accessed stored communications?				
Stored communications information received by unauthorised persons	2	-	1 suggestion	s 135(2)
Delayed certification of records for destruction	-	3[9]	-	s 150(1)
Has the agency properly applied the preservation notice provisions?				
Historic domestic preservation notices given in a successive manner	94[10]	-	1 suggestion	s 107H(1)(b)(i) s 107H(1)(b)(ii) s 107J(1)(a)(ii)
Listing the basis on which the person giving a preservation notice is authorised to do so	General finding	-	1 better practice suggestion	s 107M(1)(a)
Processes to ensure ASIC can meet the mandatory revocation requirement	General finding	-	1 better practice suggestion	s 107L(2)(a)
Preservation notices do not state a relevant condition for giving the notice	General finding	-	-	s 107J(1)(c)
Other findings				
Unable to assess stored communications information received due to destruction	2	-	-	s 117 s 150(1)

6. Crime and Corruption Commission (Queensland)

We inspected the CCC QLD from 21 to 22 November 2019 covering records for the period 1 July 2018 to 30 June 2019. We made **7 suggestions** and **2 better practice suggestions** and sent the CCC QLD a report outlining our findings on 28 February 2020.

[9] Stored communications information from 3 ASIC investigations.

[10] 2 series of 47 consecutive historic domestic preservation notices (total of 94 preservation notices).

Table 13 – 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	22	15 (68%)
Stored communications warrants	3	3 (100%)

Progress since previous inspection

We did not make any suggestions to the CCC QLD from our previous inspection conducted in 2018–19.

Significant findings

Stored communications warrants no longer in force at the time of carrier access

We identified 2 warrants where stored communications were accessed by the carrier after the warrants expired. At the time of our inspection the relevant stored communications had not been identified and quarantined. We suggested the CCC QLD quarantine the relevant stored communications and seek confirmation from the carrier as to when stored communications were accessed under the warrant. We also suggested the CCC QLD ascertain any use and communication of the stored communications and seek advice if it had been used or communicated. We further suggested the CCC QLD introduce further controls into its screening process to ensure it can identify instances where stored communications are accessed by the carrier after a warrant has expired.

The CCC QLD advised our Office the stored communications had been quarantined, no use or communication occurred and that it updated its screening procedures to mitigate future risk.

Using, communicating, and recording stored communications

We identified that the CCC QLD's use and communication registers, which the CCC QLD uses to meet the requirements under s 151(1)(h) of the Act, were incomplete for all 3 warrants inspected. As such, we were not satisfied the CCC QLD had met its record-keeping requirements in these instances. The CCC QLD advised that it has implemented processes to ensure the registers have been updated.

Conditions for giving preservation notices

Under s 107J(1)(c) of the Act a domestic preservation notice may be given if the agency considers there are reasonable grounds for suspecting that there are stored communications that might assist in connection with the investigation. The specific conditions that need to be met under s 107J(1)(c) of the Act include that the stored communications are within the relevant period for the notice, there are stored communications in existence, or might come into existence, that might assist in connection with the investigation and relate to the person or telecommunications service specified in the notice.

We identified the CCC QLD's request forms for preservation notices did not contain sufficient information to assist the authorised officer in considering whether the conditions for giving a preservation notice under s 107J(1)(c) of the Act were met. Namely, information to confirm how the service number came to notice and linked to the person of interest and how the offence under investigation relates to the use of the service. As a matter of better practice we suggested the CCC QLD advise requesting officers to include sufficient background information in the request form to assist the authorised officer to determine whether the conditions at s 107J(1)(c) of the Act are met prior to giving the preservation notice. The CCC QLD advised that it reviewed its templates to

ensure that sufficient information will be provided to assist authorised officers to determine whether the conditions for giving a preservation notice were met.

Table 14 – 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?				
Stored communications warrant accessed by carrier after warrant ceased to be in force	2	-	3 suggestions	s 119(1)
Has the agency properly managed accessed stored communications?				
Confirming who received stored communications under s 135	General finding	-	1 better practice suggestion	s 135(2)
Has the agency properly applied the preservation notice provisions?				
Preservation notices not revoked	-	2	-	s 107L(2)(a)(ii)
Wording on preservation notices	General finding	-	-	s 107H(1)(b) s 107J(1)(a)
Has the agency satisfied certain record keeping obligation?				
Retaining authoritative versions of preservation notices	3	-	1 suggestion	s 151(1)(a)
Keeping records demonstrating whether each preservation notice was properly given	General finding	-	1 better practice suggestion	s 107J(1)(c) s 151(1)(a)
Use and communication register not maintained	3	-	1 suggestion	s 151(1)(h)
Inaccuracies in reporting to the Minister	2	-	2 suggestions	s 159

7. Corruption and Crime Commission (Western Australia)

We inspected the CCC WA from 19 to 23 August 2019 covering records for the period 1 July 2017 to 30 June 2019. We did not make any recommendations or suggestions and sent the CCC WA a report noting the CCC WA's progress since our last inspection.

Table 15 – Stored communications inspection statistics: Corruption and Crime Commission (Western Australia)

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	1	1 (100%)
Ongoing domestic preservation notices	2	1 (50%)
Stored communications warrants	1	1 (100%)
Destruction of stored communications information	5	5 (100%)

Progress since previous inspection
We did not make any suggestions to the CCC WA from our previous inspection conducted in 2017–18 .

Significant findings
There were no compliance or administrative findings to report arising from our inspection.

8. Department of Home Affairs

We inspected the Department of Home Affairs (the Department) from 24 to 26 February 2020 covering records for the period 1 July 2018 to 30 June 2019. We made **5 suggestions** and **2 better practice suggestions** and sent the Department a report outlining our findings on 20 July 2020.

Table 16 – Stored communications inspection statistics: Department of Home Affairs

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	10	10 (100%)
Stored communications warrants	9	9 (100%)
Destruction of stored communications information	10	10 (100%)

Progress since previous inspection
Our previous inspection of the Department was conducted in 2018–19 covering records for the period 1 July 2017 to 30 June 2018. We made 9 suggestions to the Department. During our previous inspection we were unable to assess stored communications accessed in 2 instances as the discs containing the information were password protected. In each instance the Department could not locate the passwords to access the stored communications. During our 2019–20 inspection the Department remained unable to provide a password for one of these files. We made a further suggestion that the Department take steps to ensure all records are accessible to enable assessment of compliance at future inspections. The Department advised that it has updated its record-keeping processes.

We identified several issues from our previous inspection during this inspection noting all records inspected pre-dated our previous report being provided to the Department. This included instances where destruction of copies of stored communications was not conducted in accordance with s 150(1) of the Act and stored communications warrants were issued in the name of the subscriber not the person of interest.

Significant findings
Stored communications warrants that were expired at the time of carrier access
The Department disclosed one instance where the carrier accessed stored communications after the relevant warrant expired. The issue was identified by the Department on the day the stored communications were received from the carrier. The Department quarantined all stored communications, and the unlawfully accessed information was not used or communicated. We are satisfied with the remedial action taken by the Department in this instance and that the Department has processes in place to identify instances where stored communications may be accessed by a carrier after the relevant warrant has expired.

Multiple historic domestic preservation notices given, and stored communications warrants issued in relation to the same service/person

The Department disclosed 2 instances where it gave 2 historic domestic preservation notices in relation to the same telecommunications service to the same carrier. The subsequent historic domestic preservation notices were given to obtain stored communications that came into existence in the intervening period of approximately one week. In these instances, we did not consider that the Department returned to its previous practice of issuing historic domestic preservation notices in a successive manner, contrary (in our view) to the intended operation of the Act. However, we reiterated our position regarding the practice of giving historic domestic preservation notices in a successive manner to the Department to assist in ensuring this practice does not recommence.

Relatedly, in both instances the Department was subsequently issued with 2 stored communications warrants covering the same person (4 warrants in total). Only one warrant per person was executed, and the other 2 warrants were revoked. Obtaining more than one warrant creates a risk that an agency may not comply with the requirement under s 119(5) of the Act that a warrant must not be issued within 3 days of a previous stored communications warrant being executed relating to the same telecommunications service. To mitigate this risk we made a better practice suggestion for the Department to include a statement on its affidavits for stored communications warrants regarding whether any previous warrants are issued in relation to the same person or telecommunications service or whether multiple applications exist. The Department advised it updated its standard operating procedures.

Prescribed form of stored communications warrants

We identified 5 instances where stored communications warrants issued to the Department were not in the prescribed form as they were issued in respect of a person and related service numbers. A stored communications warrant can only be issued in respect of a person. We also identified an inconsistent approach to either omitting or striking through non-applicable paragraphs across the 5 warrants. We made a better practice suggestion for the Department to strike out non-applicable paragraphs or state nil for the conditions and restrictions paragraphs rather than omitting them entirely. The Department accepted this better practice suggestion.

Stored communications warrant certified before being issued

Section 121 of the Act requires a certified copy of a stored communications warrant to be given to an authorised representative of the carrier that holds the stored communications. The Department disclosed 4 instances where a stored communications warrant was certified before the issuing authority signed the warrant. We consider that a warrant can only be certified after the issuing authority has issued it. As such, we were concerned the warrants may have been invalidly certified and not given to the carrier in accordance with the requirements of s 121 of the Act and may have impacted any evidentiary certification under s 131 of the Act.

We suggested the Department obtain advice on the validity of these stored communications warrants. Pending the outcome of this advice we suggested the Department quarantine any stored communications obtained under these warrants. We also suggested the Department only certify a stored communications warrant after an issuing authority issued a warrant and evidenced this decision with their signature on a form that meets the requirements of s 118(1) of the Act. The Department advised it sought advice and updated its procedures and warrant template in line with our suggestions.

Table 17 – Inspection findings: Department of Home Affairs

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Prescribed form of stored communications warrants	5	-	1 better practice suggestion	s 110(1) s 118(1) Form 6
Stored communications warrant certified before being issued	-	4	2 suggestions	s 118(1) s 121 s 131
Templates for certifying warrants	4	-	-	
Legacy issue: Stored communications warrant issued in the name of the subscriber not the person of interest	2	-	1 suggestion	s 116 s 117
Stored communications warrant accessed by carrier after warrant ceased to be in force	-	1	-	s 119(1)
Legacy issue: Exercise of authority conferred by the stored communications warrant	4	-	-	s 127
Stored communications warrants issued in relation to the same service/person	-	2	1 better practice suggestion	s 119(5)
Has the agency properly managed accessed stored communications?				
Destructions occurred without chief officer approval	All copies of stored communications	-	1 suggestion	s 150(1)
Has the agency properly applied the preservation notice provisions?				
Multiple historic domestic preservation notices	-	2	-	s 107H(1)(b) s 107J(1)(a)(ii)
Other findings				
Unable to assess stored communications information	1	-	1 suggestion	-

9. Independent Broad-based Anti-corruption Commission

We inspected IBAC from 2 to 3 October 2019 covering records for the period 1 July 2017 to 30 June 2019. We made **one suggestion** and **one better practice suggestion** and sent IBAC a report outlining our findings on 2 April 2020.

Table 18 – Stored communications inspection statistics: Independent Broad-based Anti-corruption Commission

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	1	1 (100%)
Ongoing domestic preservation notices	17	8 (47%)
Stored communications warrants	4	4 (100%)
Destruction of stored communications information	3	3 (100%)

Progress since previous inspection

Our previous inspection of IBAC in 2017–18 did not identify any compliance issues.

Significant findings

Conditions for giving preservation notices

IBAC disclosed 3 instances where ongoing domestic preservation notices were given to a carrier while existing preservation notices were in force for the same telecommunications service contrary to a condition for giving an ongoing domestic preservation notice under s 107J(1)(e) of the Act. IBAC advised it believed this occurred due to a misunderstanding from staff that further ongoing domestic preservation notices should be sought 29 days after the notices came into force. IBAC took remedial action upon identifying that it incorrectly issued the notices including reviewing procedural documents, disseminating new guidelines, and updating templates.

A stored communications warrant authorises an agency to access, subject to any conditions or restrictions, all stored communications held by the carrier that were made or intended to be received by the person in respect of whom the warrant was issued before the warrant is first executed. However, in these circumstances we were unable to determine whether the stored communications were held by the carrier and therefore accessible under the warrant had the carrier not preserved the stored communications under invalid preservation notices. We suggested that IBAC seek advice to determine whether the stored communications obtained under these warrants were lawfully accessed noting the stored communications were preserved under invalid preservation notices. If the stored communications were not lawfully accessed, IBAC should quarantine the information and seek further advice regarding any use or communication of the information.

Table 19 – Inspection findings: Independent Broad-based Anti-corruption Commission

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Has the agency properly applied the preservation notice provisions?				
Ongoing domestic preservation notices given to the same carrier covering the same person	-	3	1 suggestion	s 107J(1)(e) s 107K(b) s 117
Specifying the legislative basis for offences	4	3	1 better practice suggestion	s 107J(1)(b)
Has the agency satisfied certain record keeping obligations?				
Destruction report to Minister	1	-	-	s 150(2)

10. Independent Commissioner Against Corruption (New South Wales)

We inspected the ICAC NSW from 10 to 13 March 2020 covering records for the period 1 July 2017 to 30 June 2019. We made **8 suggestions** and **one better practice suggestion** and sent the ICAC NSW a report outlining our findings on 25 June 2020.

Table 20 – Stored communications inspection statistics: Independent Commission Against Corruption (New South Wales)

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	7	6 (86%)
Ongoing domestic preservation notices	7	6 (86%)
Stored communications warrants	7	7 100%)
Destruction of stored communications information	1	1 (100%)

Progress since previous inspection

Our previous inspection of ICAC NSW in 2017–18 did not identify any compliance issues.

Significant findings

Destruction of stored communications

We identified an inconsistency between the ICAC NSW's policy and its practices regarding the process for destroying copies of stored communications information. We considered this may result in inadvertent destruction of copies of stored communications not in accordance with the Act. We suggested the ICAC NSW clarify its policy on destructions to ensure they are conducted consistently. This should include creating additional guidance on what needs to be destroyed and implementing a mechanism to accurately track and locate stored communications across all systems. The ICAC NSW advised that its policy will be updated and accurate recording in its use of stored communications register will assist with identifying copies that are required for destructions.

We also identified one instance where the chief officer certified records associated with a warrant for destruction, however, stored communications received via email were not destroyed. This meant the destruction of all stored communications was not undertaken forthwith. We identified that the ICAC NSW's practice did not demonstrate the chief officer had turned their mind to the considerations set out in s 150(1) of the Act before certifying the stored communications information for destruction. ICAC NSW's template for destruction certification under s 150(1) of the Act required an investigator to decide whether stored communications are not required rather than the chief officer. We suggested the ICAC NSW amend its process to ensure destructions are undertaken with the chief officer being satisfied the stored communications are not required for a permitted purpose in line with s 150(1) of the Act. The ICAC NSW advised our Office that its destruction form would require amendments to reflect the chief officer is satisfied the stored communications are not required.

Using, communicating, and recording stored communications

In 4 instances we identified there was no detailed information regarding use and communication of stored communications received in the ICAC NSW's use and communications logs. The ICAC NSW advised that investigators did not complete the use and communication log in these 4 instances as they considered the information was captured under a generic statement included in ICAC NSW's use and communication logs. The generic statement is that lawfully accessed information was used for the purpose of the investigation of an offence and to support the exercise of powers by the ICAC Commissioner and delegates. It is difficult to assess that use and communication of the stored communications is compliant with the Act when there is no specific information in the use and communication log. It is also difficult for the ICAC NSW to track the location of copies of stored communications information to fulfil destruction requirements.

In another instance there was no use and communication log present, and we were unable to assess the ICAC NSW's compliance with the record-keeping obligations under s 151(1)(h) of the Act. We suggested the ICAC NSW establish a consistent process for recording use and communication of stored communications to ensure it can satisfy its record keeping obligations under s 151(1)(h) of the Act. The ICAC NSW acknowledged that further information must be recorded and it would consider updating its policy, training, and a review of the register.

Data vetting and quarantining processes

We identified a lack of established procedures regarding the ICAC NSW's process for vetting stored communications information received to ensure the stored communications are within the parameters of a warrant. There is a risk that data vetting may not be conducted consistently and in instances where data is outside the scope of the warrant it may not be identified and quarantined from use or communication. We also identified 2 instances where we were unable to determine whether data vetting had occurred.

We suggested the ICAC NSW incorporate guidance regarding data vetting of stored communications received into its policy and procedural documents to ensure this assessment is conducted consistently. We also suggested the ICAC NSW establish a consistent mechanism for quarantining stored communications that is not within the parameters of a warrant to limit the risk of dealing with unlawful stored communications. The ICAC NSW advised it would update its instructional document to reflect the procedure being followed.

Prescribed form of stored communications warrants

We identified inconsistencies in the way the ICAC NSW omitted non-applicable paragraphs on stored communications warrants. As a matter of better practice, where the ICAC NSW identifies that any of

the relevant paragraphs of the prescribed form are not applicable, we suggested the ICAC NSW strike out the non-applicable paragraphs rather than omitting them entirely.

Need for training and practical guidance for investigators

We identified that ICAC NSW investigators do not receive specific training or guidance on their obligations when using Chapter 3 provisions. Chapter 3 of the Act imposes several obligations on an agency when using the stored communications provisions. As investigators are involved in exercising the powers it is important they have sufficient awareness of their obligations. We suggested the ICAC NSW provide training and practical guidance to investigators that specifically addresses their obligations relating to preservation notices including mandatory revocation as well as accounting for use and communication of stored communications and destruction requirements. The ICAC NSW advised that it would conduct training and prepare an instructional document for relevant staff.

Table 21 – Inspection findings: Independent Commission Against Corruption (New South Wales)

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Data vetting and quarantining processes	General finding 2	-	2 suggestions	s 117
Additional data review for emails	4	-	1 suggestion	
Prescribed form of stored communications warrants	2	-	1 better practice suggestion	s 118(1)(a) Form 6
Has the agency properly managed accessed stored communications?				
Destruction of stored communications	General finding 1	-	2 suggestions	s 150(1)
Has the agency satisfied certain record keeping obligations?				
Use and communication register	5	-	1 suggestion	s 151(1)(h)
Discrepancies in annual reporting	General finding	-	1 suggestion	s 159
Other findings				
Need for training and practical guidance	General finding	-	1 suggestion	-

11. Independent Commissioner Against Corruption (South Australia)

We inspected the ICAC SA from 24 to 27 February 2020 covering records for the period 1 July 2018 to 30 June 2019. We made **3 suggestions** and **one better practice suggestion** and sent the ICAC SA a report outlining our findings on 25 March 2020.

Table 22 – Stored communications inspection statistics: Independent Commissioner Against Corruption (South Australia)

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

Progress since previous inspection

We made one suggestion to the ICAC SA from our previous inspection conducted in 2018–19, regarding the prescribed form of warrants. During this inspection we made further suggestions regarding ICAC SA's warrant template as discussed below.

Significant findings

Prescribed form of stored communications warrants

The ICAC SA was not issued with any stored communications warrants during the inspection period.

The Act requires stored communications warrants to be in the 'prescribed form' found in Form 6 of the regulations. We identified the ICAC SA's stored communications warrant template did not include paragraph 2(e) of the prescribed form which relates to victims of serious contraventions. Including this paragraph in the ICAC SA's warrant template ensures officers consider the potential relevance of s 116(1)(da) of the Act (which relates to stored communications warrants applied for in relation to victims) when preparing a warrant on a case by case basis. In addition, it mitigates the risk that a warrant may inadvertently not include one of the mandatory fields by keeping the paragraph numbers consistent.

We suggested the ICAC SA include paragraph 2(e) in its warrant template. We suggested, as a matter of better practice, where the ICAC SA identifies paragraphs of the prescribed form are non-applicable (including paragraph 2(e)) it strike out the non-applicable paragraphs rather than delete them. The ICAC SA advised it would review its template.

Using, communicating, and recording stored communications

Noting that the ICAC SA was not issued with any stored communications warrants during the inspection period, we reviewed its policy and procedural documents to ensure the ICAC SA is well placed to meet its compliance obligations under the Act in the future. We identified the ICAC SA's stored communications policy document did not include investigator obligations for maintaining records under s 151 of the Act. We also found there was no established method at the ICAC SA for recording the use, communication and recording of stored communications information.

We suggested the ICAC SA update its policy document accordingly and consider ways it can consistently record use, communication and recording of stored communications information to ensure it is able to satisfy its record-keeping obligations under s 151(1)(h) of the Act. The ICAC SA advised that it would review its policy.

Table 23 – 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?				
Prescribed form of stored communications warrants	General finding	-	1 suggestion 1 better practice suggestion	s 118(1)(a) Form 6
Has the agency properly applied the preservation notice provisions?				
Handwritten annotations on preservation notices	1	-	-	s 107M(2)(a)
Has the agency satisfied certain record keeping obligations?				
Maintaining records for using, communicating and recording stored communications information	General finding	-	2 suggestions	s 151(1)(h)
Other findings				
Area of risk: Ensuring use of current templates	General finding	-	-	-

12. New South Wales Crime Commission

We inspected the NSW CC from 15 to 18 July 2019 covering the period 1 July 2017 to 30 June 2019.[11] We made **2 better practice suggestions** and sent the NSW CC a report outlining our findings on 28 February 2020.

Table 24 – Stored communications inspection statistics: New South Wales Crime Commission

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Ongoing domestic preservation notices	7	7 (100%)
Stored communications warrants	6	6 (100%)

Progress since previous inspection

We made one suggestion to the NSW CC at our previous inspection conducted in 2017–18, regarding a disclosure of non-compliance with the mandatory revocation requirements for preservation notices. We did not identify this issue at our 2019–20 inspection.

Significant findings

Successive warrant issued in contravention of s 119(5) of the Act

We identified one instance where a stored communications warrant was invalidly issued as it was issued within 3 days of a previous warrant being executed which related to the same person and telecommunication service in contravention of s 119(5) of the Act. The accompanying affidavit in this instance incorrectly stated the earlier warrant had not been executed. The NSW CC confirmed the stored communications obtained under this warrant were not used and were destroyed.

[11] All records inspected were in relation to the 2017–18 period.

In another instance we identified a lack of detail on the affidavit accompanying an application for a stored communications warrant regarding previous warrants issued for the same person. While this is not a legislative requirement we consider there is a risk that if the issuing authority is unaware of the details regarding any previous warrants issued for the same telecommunication service or person, a warrant may be issued contrary to s 119(5) of the Act. As a matter of better practice, to mitigate this risk we suggested the NSW CC include sufficient detail in affidavits regarding whether any previous warrants were issued in relation to the same person or telecommunication service. The NSW CC advised that its affidavit template now includes a section which requires details of any previous warrants to be included.

Table 25 – Inspection findings: New South Wales Crime Commission

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Successive warrant issued in contravention of s 119(5) of the Act	1	-	1 better practice suggestion	s 119(5)
Has the agency properly applied the preservation notice provisions?				
Preservation notice not dated	1	-	1 better practice suggestion	s 107H(1) s 107M(2)(a)

13. New South Wales Police Force

We inspected the NSW PF from 3 to 6 February 2020 covering records for the period 1 July 2018 to 30 June 2019. We made **8 suggestions** and **3 better practice suggestions** and sent the NSW PF a report outlining our findings on 22 May 2020.

Table 26 – 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	817	47 (6%)
Ongoing domestic preservation notices	92	10 (11%)
Stored communications warrants	705	58 (8%)

Progress since previous inspection

We made one suggestion and one better practice suggestion to the NSW PF at our previous inspection conducted in 2018–19, regarding determining whether stored communications were lawfully accessed and incorrect template wording in affidavits. We did not identify these issues during our 2019–20 inspection. However, we again identified an issue regarding stored communications warrants applied for in relation to a victim of a serious contravention, discussed below.

Significant findings

Affidavits to contain accurate and sufficient information

We identified 2 instances where the NSW PF applied for, obtained, and executed a stored communications warrant in relation to a person who was a victim of a serious contravention. In these instances, it was our view the affidavits did not fully explain why the NSW PF determined it

was impracticable to seek the victim's consent. We considered this could impact the issuing authority's ability to make a fully informed decision under s 116(1)(da) of the Act.

The NSW PF disclosed 7 instances, and we identified an additional instance, where affidavits accompanying stored communications warrant applications provided inaccurate information about whether there were stored communications in existence.

We suggested the NSW PF ensure that affidavits accompanying applications for stored communications warrants provide accurate and sufficient information to enable an issuing authority to make fully informed decisions, including about the matters set out in s 116(1) of the Act. Where a stored communications warrant is being sought in relation to a victim of a serious contravention we suggested the NSW PF ensure that affidavits accurately reflect whether or not consent has been sought, and if not, clearly demonstrate how the thresholds of 'unable' or 'impracticable' are met. This could be achieved through guidance on what constitutes unable or impracticable to gain consent, emphasising that consent should be obtained in all other circumstances. Such guidance should be incorporated in policy and disseminated to all staff involved in administrating stored communications at the NSW PF.

The NSW PF advised of amendments to its guidance material to improve the accuracy of information within applications for stored communications warrants and the development of guidance in relation to stored communications warrants sought in relation to victims of a serious contravention.

Affidavits not addressing whether there were previous warrants

Where a further warrant relates to the same telecommunications service as the previous warrant, s 119(5) of the Act requires that it must not be issued within 3 days after the day on which the previous warrant was executed. We identified 2 instances where affidavits accompanying stored communications warrants did not state whether there were any previous applications about the same person or telecommunications service. While this is not a legislative requirement under the Act we consider there is a risk that a warrant may be issued contrary to s 119(5) of the Act if the issuing authority is unaware of the details regarding any previous warrants issued for the same telecommunications service. These instances were contrary to the NSW PF's usual practice for an affidavit to include a statement whether there were any previous applications for the same telecommunications service. As a matter of better practice, we suggested the NSW PF remind relevant staff of this practice which the NSW PF adopted.

Prescribed form of stored communications warrants

The Act requires stored communications warrants to be in the 'prescribed form' found in Form 6 of the Regulations. We identified 3 instances where stored communications warrants issued to the NSW PF were not in the prescribed form. We also identified one warrant where the NSW PF deleted a paragraph it deemed non-applicable. As a matter of better practice, we suggested paragraphs be struck out rather than deleted where NSW PF identifies they are non-applicable. The NSW PF advised it adopted this practice.

Disclosure register

During the inspection we noted limited sharing of issues identified between the areas of the NSW PF that have responsibility for the stored communications warrant process. We also noted there is no centralised process to track and record issues as they occur. To increase awareness of contemporaneous issues concerning the operation of the stored communications regime, as a matter of better practice, we suggested NSW PF establish a system to improve its ability to identify and manage issues consistently, implement improved processes, and support transparency (for

example a centralised disclosure or issues register). The NSW PF advised it was considering this matter.

Table 27 – 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?				
Affidavits should contain accurate and sufficient information for the issuing authority to make fully informed decisions	3	7	2 suggestions	s 113 s 116(1)
Revoking stored communications warrants	General finding	-	1 suggestion	s 122(1)
Administrative errors on warrants	2	5	2 suggestions	s 117 s 118(2)
Affidavits not addressing whether there were previous warrants	2	-	1 better practice suggestion	s 119(5)
Prescribed form of stored communications warrants	4	-	1 better practice suggestion	s 118(1)(a) Form 6
Has the agency properly managed accessed stored communications?				
Stored communications sent by the carrier to the incorrect area of NSW Police	1	-	1 suggestion	s 135(2) s 151(1)(h)
Area of risk – Dissemination of stored communications via email in urgent circumstances	5	-	1 suggestion	s 150(1)
Has the agency properly applied the preservation notice provisions?				
Mandatory revocation of preservation notices	2	5[12]	1 suggestion	s 107J(1)(c) s 107K(b) s 107L(2)(a)(ii)
Was the agency cooperative and frank?				
System to identify and manage issues, and support transparency	General finding	-	1 better practice suggestion	-

14. Northern Territory Police

We inspected the NT Police from 8 to 12 July 2019 covering records for the period 1 July 2017 to 30 June 2019. We made **6 suggestions** and sent the NT Police a report outlining our findings on 18 September 2019.

[12] In 3 instances, we were satisfied the mandatory revocation provision under s 107L(2)(a) of the Act was not enlivened. In one instance the mandatory revocation provision was enlivened, and the notice should have been revoked. In another instance we were unable to determine whether the NSW Police still maintained an intention to obtain a warrant to access the stored communications, or whether the notice should be revoked.

Table 28 – Stored communications inspection statistics: Northern Territory Police

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	60	7 (12%)
Ongoing domestic preservation notices	24	1 (4%)
Stored communications warrants	6	6 (100%)
Destruction of stored communications information	26	8 (31%)

Progress since previous inspection

We made 2 suggestions to the NT Police from our previous inspection conducted in 2017–18. For one of these suggestions regarding ensuring destruction of stored communications forthwith, we identified this issue again during our 2019–20 inspection.

Significant findings

Prescribed form of warrants

For all warrants issued to the NT Police during this period we identified that the prescribed form of the warrants was not complied with. We suggested the NT Police refer to the Regulations which are in force at the time the warrant is drafted to ensure compliance with the prescribed form.

Destruction of stored communications

For all 26 warrant files destroyed by the NT Police during the period, the destructions were not conducted forthwith, contrary to s 150(1) of the Act. The destruction was not completed until approximately 11 months after the chief officer authorised the files for destruction. In one instance we identified that copies of the stored communications information remained on file at the time of our inspection. We suggested the NT Police consider updating its stored communications standard operating procedures to highlight the chief officer's obligation to cause information or records to be destroyed forthwith, and that officers responsible for conducting destructions destroy stored communications records as soon as practicable after receiving chief officer authorisation.

For 3 warrant files we were unable to determine when destruction took place and whether the records were destroyed before or after chief officer approval under s 150(1) of the Act due to a lack of records kept by NT Police. We suggested the NT Police undertake awareness-raising initiatives with investigators regarding the destruction requirements under s 150 of the Act. In 3 instances it was also unclear whether stored communications certified for destruction were destroyed or remained in the NT Police's possession. We suggested the NT Police consider implementing a process for conducting a reconciliation of all records containing stored communications held by investigators prior to obtaining the chief officer's approval.

Conditions for giving preservation notices

We identified 2 ongoing domestic preservation notices given by the NT Police to the same carrier which specified different telecommunications services but the same person, contrary to the condition for giving an ongoing domestic preservation notice under s 107J(1)(e) of the Act. There must not be another ongoing domestic preservation notice in force that was given to the same carrier and specifies the same person or same telecommunications service. We suggested strategies to the NT Police for preparing preservation notices to mitigate the risk of non-compliance with

s 107J(1)(e) of the Act. NT Police advised suggestions had been, or were in the process of being, resolved.

Table 29 – Inspection findings: Northern Territory Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Prescribed form of stored communications warrants	6	-	1 suggestion	s 118(1)(a) Form 6
Has the agency properly managed accessed stored communications?				
Stored communications records not destroyed forthwith	26	-	1 suggestion	s 150(1)
Unable to determine whether the destruction of stored communications occurred with chief officer approval	3	-	1 suggestion	s 150(1) s 151(1)(i)
Stored communications certified for destruction not accounted for	3	-	1 suggestion	s 150(1) s 151(1)(i)
Has the agency properly applied the preservation notice provisions?				
Ongoing preservation notices given to the same carrier covering the same person	2	-	1 suggestion	s 107J(1)(e)
Administrative errors on revocation instruments for preservation notices	General finding	-	1 suggestion	s 107M(1)(a)

15. Queensland Police Service

We inspected the QPS from 19 to 20 November 2019 covering records for the period 1 July 2018 to 30 June 2019. We made **3 suggestions** and **3 better practice suggestions** and sent the QPS a report outlining our findings on 30 March 2020.

Table 30 – Stored communications inspection statistics: Queensland Police Service

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	19	9 (56%)
Ongoing domestic preservation notices	220	41 (21%)
Stored communications warrants	165	45 (27%)
Destruction of stored communications information	100	38 (38%)

Progress since previous inspection

We made 2 suggestions to the QPS from our previous inspection conducted in 2018–19, regarding destruction of stored communications. We made further suggestions regarding the QPS' destructions during our 2019–20 inspection, as discussed below.

Significant findings

Destruction of stored communications

Following our previous inspection, the QPS amended its procedures to remove its internal timeframe for meeting the 'forthwith' requirement under s 150(1) of the Act to instead emphasise that destructions are to occur without delay. 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. We suggested the QPS explore further preliminary steps to be taken prior to certification by the chief officer to ensure it is positioned to destroy stored communications material within a reasonable timeframe. The QPS advised it would include additional advice to officers within instructions regarding preliminary action that can be taken.

The QPS also disclosed one instance where an investigator continued to hold stored communications following those records being certified for destruction by the chief officer. We suggested the QPS destroy the stored communications forthwith.

Keeping records that indicate whether preservation notices were properly given

We identified an absence of records kept at the QPS regarding the decision to give a preservation notice and no specific guidance around how these records are to be kept. As such, we found the QPS may not be meeting its record keeping obligations under s 151(1)(a) of the Act. As a matter of better practice, we suggested the QPS implement a consistent process to capture information that indicates whether a preservation notice was properly given. This should include information relevant to the decision to give a preservation notice such as background information on the offence under investigation and linking the telecommunications service number to the person of interest. The QPS advised it was reviewing the matter.

Table 31 – Inspection Findings: Queensland Police Service

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Content of affidavits accompanying applications for stored communications warrants	6	-	1 better practice suggestion	s 113
Prescribed form for Stored Communications Warrants	9	General disclosure	-	s 118(1)(a) Form 6
Has the agency properly managed accessed stored communications?				
Area of risk: receiving stored communications	General finding	-	1 suggestion	s 135(2)
Destruction processes and meeting a forthwith requirement	General finding	-	1 suggestion	s 150(1)
Stored communications held following	-	1	1 suggestion	s 150(1)

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
certification for destruction				
Has the agency properly applied the preservation notice provisions?				
Keeping records that indicate whether preservation notices were properly given	General finding	-	1 better practice suggestion	s 151(1)(a) s 107J(1)(c)
Has the agency satisfied certain record keeping obligations?				
Annual reporting to the Minister	1	-	1 better practice suggestion	s 150(2) s 159

16. South Australia Police

We inspected the SA Police from 2 to 6 September 2019, covering records for the period 1 July 2017 to 30 June 2019. We made **one suggestion** and **one better practice suggestion** and sent the SA Police a report outlining our findings on 3 April 2020.

Table 32 – Stored communications inspection statistics: South Australia Police

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	161	26 (16%)
Ongoing domestic preservation notices	47	7 (15%)
Stored communications warrants	43	32 (74%)

Progress since previous inspection

We made one suggestion to the SA Police at our previous inspection conducted in 2017–18, regarding stored communications that did not comply with warrant restrictions. During our 2019–20 inspection, we were satisfied that SA Police had processes in place to identify and manage access to unauthorised stored communications however we made a further suggestion regarding effective quarantining.

Significant findings

Data vetting and quarantining processes

We identified one instance where stored communications information was provided by the carrier outside of the date range restriction on the warrant. While the SA Police attempted to redact the information received, we found it had used an ineffective redaction methodology. We suggested the SA Police ensures it effectively quarantines all unlawfully obtained stored communication information and confirms the quarantined information was not used or communicated. The SA Police advised that training and updated guidance documents were provided to ensure that data is effectively quarantined and enquiries were being undertaken to locate all copies of the stored communications. The SA Police also advised the stored communications would not be further communicated.

Affidavits not addressing whether there were previous warrants

Where a further warrant relates to the same telecommunications service as the previous warrant, s 119(5) of the Act requires it must not be issued within 3 days after the day on which the previous warrant was executed. We found the SA Police's affidavits accompanying stored communications

warrants did not address whether a previous warrant had been issued in respect of the same person or telecommunications service. While this is not a legislative requirement under the Act, we consider there is a risk that a warrant may be issued contrary to s 119(5) of the Act if the issuing authority is unaware of the details regarding any previous warrants issued for the same telecommunications service. As a matter of better practice, we suggested the SA Police implement a consistent practice to include details in affidavits for stored communications warrants regarding whether any previous warrants were issued in relation to the same person or telecommunications service. The SA Police advised of changes to its template and policy documents.

Table 33 – Inspection Findings: South Australia Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Quarantining accessed stored communications not authorised by a warrant	1	-	1 suggestion	s 117
Addressing whether there were previous warrants	General finding	-	1 better practice suggestion	s 119(5)
Has the agency properly applied the preservation notice provisions?				
Practice of notifying carriers of preservation notices	3	-	-	s 107H(1) s 107J(1) s 107K(a)
Partial revocation of preservation notice	1	-	-	s 107L(1) s 107K(b)(ii) s 107L(3)

17. Tasmania Police

We inspected Tas Police from 25 to 29 November 2019, covering records for the period 1 July 2018 to 30 June 2019. We made **4 recommendations** about Tas Police's overall approach to compliance (as discussed in Part B of this report) and made **2 recommendations, 9 suggestions** and **one better practice suggestion** about its access to stored communications. We sent Tas Police our final report on 21 December 2020.

Table 34 – Stored communications inspection statistics: Tasmania Police

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	15	2 (13%)
Ongoing domestic preservation notices	127	16 (13%)
Stored communications warrants	50	14 (28%)
Destruction of stored communications information	77	34 (44%)

Progress since previous inspection

We made 2 recommendations, 10 suggestions and 1 better practice suggestion to Tas Police at our previous inspection conducted in 2018–19. We found that, while Tas Police had acted on some of

our previous findings, it had not adequately addressed many of the issues highlighted at our previous inspection.

Significant findings

Data vetting and quarantining processes

We identified several instances where Tas Police had not effectively quarantined unlawfully accessed stored communications. In these instances (some of which were identified by our Office during previous inspections), electronic files for the records were quarantined but hardcopy files were not quarantined.

We identified that, while Tas Police undertakes data vetting of stored communications it receives, the nature of the checks conducted is not recorded against a checklist or document. In the absence of established procedures, there is a risk that data vetting may not be performed consistently or at all and, where data is outside the scope of the warrant, it may not be identified and quarantined from use, communication or recording.

We recommended that Tas Police establish:

- clear and effective procedures to support its staff to consistently vet stored communications it receives and record the results, to ensure that what a carrier has provided is within the authority of the warrant
- a consistent mechanism for quarantining unlawfully accessed stored communications to limit the risk of dealing with unlawful stored communications. This mechanism should include appropriate quarantining of both electronic and hardcopy files so that anyone reviewing a file is aware the stored communications must not be used, communicated, or recorded.

We also suggested that Tas Police should quarantine the relevant stored communications on both electronic and hard copy files.

Remedial action on stored communications warrants in relation to a victim

We previously identified instances where stored communications warrants were issued to Tas Police in relation to a victim of a serious contravention, where either the victim did not consent or was not provided the opportunity to consent. During this inspection, Tas Police disclosed an instance where a preservation notice was given, where available information indicated that Tas Police was seeking the stored communications of both the witness and the victim of a serious contravention. While this preservation notice was revoked and s 116(1)(da) of the Act does not apply when giving preservation notices, it indicates Tas Police contemplated accessing the stored communications of a victim and highlights a lack of awareness at Tas Police regarding the relevant considerations under the Act. Tas Police informed our Office that it circulated advice to investigating officers about their requirements under the Act and will incorporate a clear position in relation to this matter in its Standard Operating Procedures (SOPs).

Destruction of stored communications

During this inspection we did not see any changes to Tas Police's destruction processes, following suggestions made in our previous report, and found there were insufficient records to confirm what stored communications were destroyed and when destruction took place. As a result, we were not satisfied that Tas Police complied with its record-keeping obligation under s 151(1)(i) of the Act. We were also unable to verify whether destructions were completed 'forthwith', as required under s 150(1) of the Act. In its response to our 2018–19 report, Tas Police told us it had amended its destructions process, and its SOPs would be updated to include enhanced process guidelines to

ensure destructions are conducted consistently with s 150 of the Act. We will review these changes at our next inspection.

We also identified one instance where available records showed particular stored communications were not destroyed 'forthwith', and Tas Police disclosed an instance where destruction was not fully completed as a copy of the stored communications had been retained by an investigator. We suggested that Tas Police destroy relevant stored communications forthwith.

We also suggested that Tas Police ensure that its destructions process includes a mechanism for ensuring that all product has been destroyed before deciding the destruction is complete. As a matter of better practice, we suggested that Tas Police considers measures to ensure that investigators assess whether stored communications information is likely to be required for a permitted purpose prior to requesting chief officer approval for the information to be destroyed.

Conditions for giving preservation notices

Under s 107J(1)(c) of the Act, a domestic preservation notice may be given if the agency considers there are reasonable grounds for suspecting that, in the relevant period for the notice, there are stored communications in existence or might come into existence that might assist in connection with the investigation, and relate to the person or telecommunications service specified in the notice.

We identified instances where applications for a preservation notice did not contain sufficient information to assist the person giving the notice to determine whether the conditions under s 107J(1)(c) of the Act were met. We were not satisfied that Tas Police had met its obligation under s 151(1)(a) of the Act to keep records indicating whether a preservation notice was properly given. Due to the lack of record keeping, we also could not be satisfied the conditions for giving the preservation notices under s 107J(1)(c) were met. All 3 preservation notices were later revoked due to an unrelated administrative error identified on the forms. We suggested that Tasmania Police ensure that applications for preservation notices include sufficient background information to assist the person giving the preservation notice to determine whether the conditions at s 107J of the Act are met.

Table 35 – Inspection findings: Tasmania Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Identifying and managing unlawfully accessed stored communications	General finding 6	2	2 recommendations 1 suggestion	s 117
Remedial action on stored communications warrants in relation to a victim	2	1	1 suggestion	s 113 s 116(1)(da)
Has the agency properly managed accessed stored communications?				
Unable to confirm if destructions occurred forthwith	General finding	-	-	s 150(1)
Incomplete destruction	-	1	2 suggestions 1 better practice suggestion	
Destruction not undertaken forthwith	1	-	1 suggestion	

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Has the agency properly applied the preservation notice provisions?				
Conditions for giving ongoing preservation notices	3	-	1 suggestion	s 107J(1)(c) s 151(1)(a)
Incorrect legislative references and wording on preservation notice templates	General finding	-	2 suggestions	s 107H(1) s 107H(1)(b)(ii) s 107K(b) s 107M
Has the agency satisfied certain record keeping obligations?				
Reporting obligations	General finding	-	1 suggestion	s 159

18. Western Australia Police

We inspected the WA Police from 5 to 9 August 2019, covering records for the period 1 July 2018 to 30 June 2019. We made **one suggestion** and **one better practice suggestion** and sent the WA Police a report outlining our findings on 20 February 2020.

Table 36 – Stored communications inspection statistics: Western Australia Police

Stored communications inspection statistics		
Type of records	**Records made available**	**Records inspected**
Historic domestic preservation notices	74	14 (19%)
Ongoing domestic preservation notices	71	15 (21%)
Stored communications warrants	48	20 (42%)
Destruction of stored communications information	34	34 (100%)

Progress since previous inspection

We did not make any suggestions to the WA Police from our previous inspection conducted in 2018–19 and did not identify reoccurring issues.

Significant findings

Destruction of stored communications

We identified 10 instances where the WA Police's destruction of stored communications records was not forthwith as required by s 150(1) of the Act, in light of WA Police's advice during the inspection that it considers 'forthwith' to be less than 2 weeks. This timeframe was exceeded by approximately one week in these 10 instances. We also identified 6 instances where the chief officer authorised stored communications records for destruction, however, we were unable to determine if all stored communications were destroyed. We suggested the WA Police review its destruction process and implement a process to locate all stored communications records/information in its possession.

For the 10 instances we identified where destruction was not forthwith, the WA Police advised that it considered 3 weeks was reasonable in the circumstances. The WA Police advised it would endeavour to complete destructions within 2 weeks moving forward. The WA Police also advised it had updated standard operating procedures and implemented measures to increase the onus on investigators to account for all stored communications.

Prescribed form of stored communications warrants
The Act requires stored communications warrants to be in the 'prescribed form' found in Form 6 of the Regulations. We identified during the inspection the WA Police's practice was to delete paragraph 2(b) under Item 1 of Form 6 of the Regulations from the warrant when not applicable. This altered the paragraph numbers on the warrant so it no longer aligned with the prescribed form.

We suggested the WA Police, as a matter of better practice, strike through non-applicable paragraphs rather than deleting them. This ensures the paragraphs on the warrant align with the prescribed form and mitigates the risk that a warrant inadvertently does not comply with the prescribed form.

Table 37 – Inspection findings: Western Australia Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Is the agency only dealing with lawfully accessed stored communications?				
Prescribed form of warrant	General finding	-	1 better practice suggestion	s 118(1)(a) Form 6
Revocation of stored communications warrant when no longer required	1	-	-	s 119(1) s 122(1)
Has the agency properly managed accessed stored communications?				
Stored communications not destroyed forthwith	10	-	1 suggestion	s 150(1)
Unable to confirm destruction	6	-		

Part D – Telecommunications data

Telecommunications data and the Commonwealth Ombudsman's oversight function

Under s 186B(1)(b) of the *Telecommunications (Interception and Access) Act 1979* (the Act), the Ombudsman must inspect the records of an enforcement agency to determine the extent of compliance with Chapter 4. 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.

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 the content of a communication is sought.

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 a session
- the start and finish time of each IP session
- the amount of data uploaded/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).

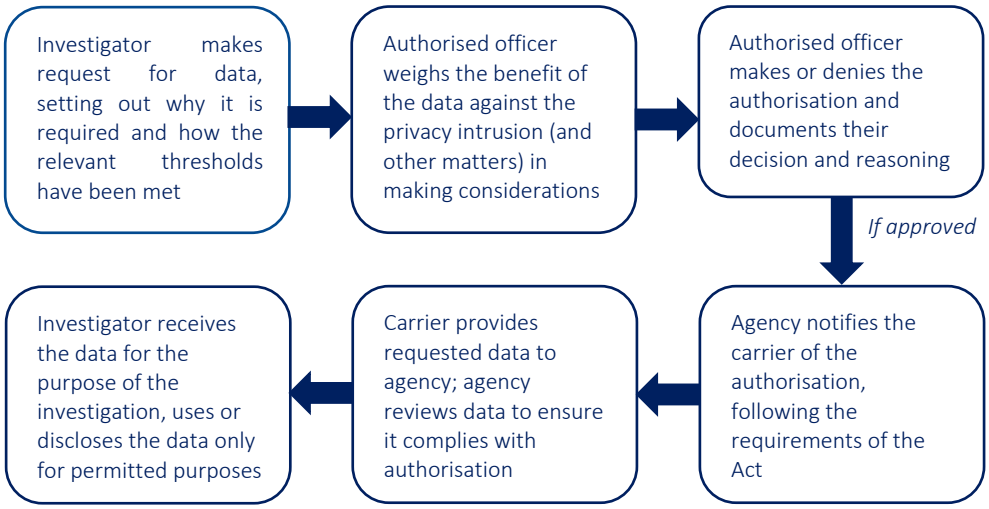
To authorise disclosure of telecommunications data, amongst other considerations, an agency must weigh the likely relevance and usefulness of the disclosed telecommunications data to the investigation against the privacy intrusion it causes.

Our Office does not review the merits of a decision to authorise disclosure of data. We assess whether agencies satisfy the requirements of the Act which involves assessing there is sufficient information for officers authorising these disclosures 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 by authorising the disclosure of telecommunications data under Chapter 4 of the Act is made by the agency investigating and not an external issuing authority.

Enforcement agencies may authorise the disclosure of telecommunications data that already exists, known as a historic authorisation. An enforcement agency that is a criminal law-enforcement agency under the Act may also authorise telecommunications data that comes into existence when an authorisation is in force, known as a prospective authorisation. A prospective authorisation may be in force for a maximum period of 45 days from when the authorisation is made.

Only officers authorised by the chief officer of an agency can authorise disclosure of telecommunications data. Figure 1 below outlines a typical authorisation process.

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



We inspect a sample of both historic and prospective authorisations. We look at the background material in the request documents, to be satisfied 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, including that agencies maintain records demonstrating that any disclosure or use of telecommunications data complied with the requirements of the Act. We assess the agency's compliance with the Act by looking at individual files in detail alongside the processes, guidance, and general approach of an agency to complying with Act.

Summary of telecommunications data findings

During 2019–20 our Office inspected 18 agencies' access to telecommunications data under Chapter 4 of the Act. In most instances our inspections covered records for the period 1 July 2018 to 30 June 2019. In 8 instances, where we did not conduct inspections of agencies during 2018–19, we also inspected records for the period 1 July 2017 to 30 June 2018 (see table 39).

While some agencies demonstrated a high level of compliance with the Act there were some instances where we identified issues leading to our Office making recommendations and suggestions related to those agencies' compliance frameworks. Agencies with the highest number of compliance issues identified, typically police forces and larger agencies, were also responsible for the highest number of telecommunications data authorisations as highlighted in table 38 below.

Maintaining a sufficient level of awareness of the Act's requirements for those exercising the powers is an ongoing challenge. We note considerable differences in awareness and compliance between agencies that do not provide regular and tailored compliance training and agencies that do. Typically, larger agencies have greater numbers of requesting and authorised officers (who may be geographically dispersed). This makes sufficient training and guidance critical to achieving compliance with the Act. Where identified as a contributing factor to compliance issues, we continue to make recommendations and suggestions to implement adequate and effective training.

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

Agencies not inspected in relation to Chapter 4 of the Act during 2019–20
As a result of COVID-19 restrictions our Office was required to temporarily pause inspections in mid-March 2020. As a result, we did not inspection all agencies' compliance with Chapter 4 of the Act. We did not conduct inspections at the LECC and IBAC.

We will inspect a sample of these 2 agencies' records that were unable to be completed at our 2020–21 inspections.

Recommendations and suggestions made during 2019–20
A recommendation reflects a serious compliance issue. A suggestion reflects less serious and/or isolated issues where we consider an agency should take action to improve. Better practice suggestions highlight ways an agency might refine its practices where existing practice may expose the agency to a risk of non-compliance.

Table 38 – Number of recommendations, suggestions, better practice suggestions made per agency during the 2019–20 inspection period from telecommunications data inspections

Agency	Recommendations	Suggestions	Better practice suggestions
ACCC	-	5	3
ACIC	-	5	1
ACLEI	-	7	3
AFP	-	13	3
ASIC	-	4	4
CCC QLD	-	4	3
CCC WA	-	3	3
Home Affairs	3	20	3
IBAC	Not inspected		
ICAC NSW	-	9	1
ICAC SA	-	10	8
LECC	Not inspected		
NSW CC	-	4	-
NSW PF	9	12	2
NT Police	-	16	-
QPS	-	12	8
SA Police	-	12	3
Tasmania Police	3	13	-
Victoria Police	-	10	2
WA Police	-	5	1
TOTAL:	**15**	**164**	**48**

Table 39 – Use of telecommunications data powers and records inspected in the 2019–20 period

Agency	Records period inspected	Total Historic	Historic Inspected	Total Prospective	Prospective inspected	Total inspected
ACCC	17–18, 18–19	169	56	-	-	56
ACIC	18–19	6,555	31	1,279	43	74
ACLEI	17–18, 18–19	773	93	252	65	158
AFP	18–19	17,268	83	4,711	30	113
ASIC	18–19	1,822	40	37	13	53
CCC QLD	18–19	1,015	43	225[13]	30	73
CCC WA	17–18, 18–19	247	83	162	72	155
Home Affairs	18–19	3,321	50	225	44	94
ICAC NSW	17–18, 18–19	589	35	94	17	52
ICAC SA	17–18, 18–19	508	65	56	28	93
NSW CC	17–18, 18–19	6,216	50	2,325	58	108
NSW Police	18–19	110,162	39	1,062	41	80
NT Police	17–18, 18–19	4,019	85	658	93	178
QPS	18–19	23,895	62	4,252	61	123
SA Police	17–18, 18–19	11,629[14]	122	763	107	229
Tasmania Police	18–19	5,979	29	185	41	70
Victoria Police	18–19	93,893	57	11,898	54	111
WA Police	18–19	23,397	54	2,117	42	96
TOTAL:		**311,457**	**1,077**	**30,301**	**839**	**1,916**

[13] The actual number of prospective authorisations is lower than reported as revocations were also counted as authorisations in several instances.

[14] These figures were reported for the 2017–18 historic records as "3830 / 5793". They may not be accurate for reasons that are discussed further in the body of the report.

The AFP also made authorisations issued under Journalist Information Warrants (JIWs) and authorisations for telecommunications data on behalf of foreign countries.

Table 40 – Number of AFP authorisations issued under JIWs (that have not been previously inspected by our Office) and number of AFP authorisation for telecommunications data on behalf of foreign countries

JIWs	JIW authorisations	JIW authorisations inspected	Foreign Historic	Foreign Historic Inspected	Foreign Prospective	Foreign Prospective Inspected	Total inspected
-	14[15]	14	43	18	0	-	**32**

Compliance issues and compliance risks

This section provides a brief overview of the significant issues we identified across most agencies during our 2019–20 inspections and the compliance risks they create. More detail on the specific circumstances at each agency can be found in the telecommunications data findings section. We continued to monitor these issues closely on our 2020–21 inspections.

Data vetting and quality control frameworks

There is always a risk that data will be received from a carrier outside the parameters of a telecommunications data authorisation. A robust data vetting and quality assurance framework is vital to ensuring that all data received by an agency is within the parameters of the authorisation and that any data received outside the authorisation parameters is managed appropriately. If unlawfully accessed telecommunications data is not identified it may be used or disclosed without proper authority including in prosecutions or other legal proceedings.

We consider it essential that all agencies exercising telecommunications data powers under Chapter 4 of the Act have formal processes, policies and staff training in place for vetting and appropriately managing telecommunications data. At a minimum these data vetting processes should include confirming:

- the data received relates to the service number listed on the authorisation
- the data received is the type of data requested in the authorisation
- the data received is within the time and date range specified on the authorisation
- no content has been received.

Generally, where agencies displayed an effective data vetting and quality control framework, they included:

- a central compliance team that receives, vets, and manages all telecommunications data received from carriers prior to its dissemination to investigators

[15] The number here reflects the number of authorisations issued under JIWs during this period that were not previously inspected by our Office 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. These 14 authorisations were not inspected at that time as the warrant under which they were made was still in force at the time of the inspection. The inspection scope included only authorisations made under an expired or revoked journalist information warrant. All remaining JIWs and corresponding authorisations were inspected during the September 2018 non-routine inspection. www.ombudsman.gov.au/__data/assets/pdf_file/0021/78123/Commonwealth-Ombudsman-AFP-JIW-report-PDF-FOR-WEBSITE.pdf

- detailed guidance material, including policies and processes for vetting, identifying, and managing all telecommunications data received
- training for compliance staff in all aspects of data vetting, quarantining and management.

Data vetting practices at police forces
During the 2019–20 inspections we found that many police forces did not have adequate policies or processes in place to vet and quarantine the telecommunications data they received from carriers. This included instances where a quarantining procedure was in place but was undermined by the lack of a consistent process to identify unauthorised data or no formalised guidance on the process to be undertaken.

Many police forces do not have a central compliance team to undertake data vetting. In these circumstances responsibility for data vetting sits with individual investigators working in the numerous teams exercising the powers. Our inspections found this often results in inconsistent data vetting and management processes in an agency, especially when coupled with an absence of policy or guidance material. It is a compliance risk where investigators are given the responsibility to vet any telecommunications data but are not instructed how to effectively perform the vetting.

Investigators may not have the same familiarity with telecommunications provider datasets as dedicated compliance areas. As such decentralised data vetting is only practicable and effective when clear and effective guidance is readily available and supplemented by appropriate compliance-focused training.

Journalist information warrant controls
Under s 180H of the Act, unless a JIW is in force, an authorised officer must not make an authorisation that would disclose information or documents relating to a particular person if:

- the authorised officer knows or reasonably believes that person to be a journalist or an employer of the journalist
- a purpose of making an authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source.

During our 2019–20 inspections we assessed all agencies on whether they had effective controls and procedures in place to ensure that requesting and authorised officers were prompted to assess if the circumstances of the authorisation involved a journalist and when so, to seek legal advice as appropriate.

We reviewed multiple elements of agencies' processes covering:

- policies and procedures, such as SOPs, with an emphasis on the availability of practical guidance
- templates and processes with an emphasis on embedded controls
- training materials
- knowledge of staff exercising the powers such as requesting and authorised officers.

We found that while many agencies were generally aware of the JIW requirements there was a lack of detailed guidance around the necessary actions to take when journalist involvement was identified. We also found an absence of in-built controls requiring officers to turn their minds to assess the existence of journalist involvement in the authorisation request. Compulsory prompts would assist in mitigating unauthorised access to telecommunications data involving a journalist.

Seniority of authorised officers

The role of the authorised officer is a critical control for ensuring that telecommunications data powers are used appropriately. Most Australian government agencies we inspect set the minimum level of authorised officer at Executive Level 2 and occasionally at Executive Level 1 (or equivalent level).

However, Case study 1 provides an example where this provision resulted in more junior officers (below Executive Level or equivalent) being made authorised officers.

It is our view that it is inappropriate for an officer below Executive Level 1 (or equivalent) to undertake the role and responsibility of an authorised officer. First, the legislation requires authorised officers to occupy a 'management office or management position' as set out in s 5AB(1) of the Act. We do not consider that a more junior officer performs a 'management position' in the context of telecommunications data authorisations even in cases where a junior officer may supervise even more junior staff in a particular team. Second, the general risks created by the insufficient training and guidance material available to authorised officers that we identified are heightened when junior and less experienced staff occupy the authorised officer role.

The authorised officer role should be one of sufficient autonomy and seniority to enable the authorised officer to make independent decisions that are informed by experience, access to information and a close understanding of legislative obligations.

Case study 1 – Department of Home Affairs

During our inspection of the Department we identified significant issues relating to the seniority of authorised officers. During the inspection period 6 different officers performed the role of authorised officer at the APS 6 level. Many acted in the role for short periods of time. Most of the department's telecommunications data authorisations are signed by a single APS 6 officer.

Based on the inspection we consider that APS 6 level officers are not sufficiently senior to meet the requirements of 'management office or management' position as set out in s 5AB(1) of the Act regardless of whether the APS 6 officer supervises junior staff. There are significant risks associated with authorising APS 6 level authorised officers which are further heightened when APS 6 positions are temporarily filled by acting APS Level 5 officers. The lack of training, policy and procedure or guidance available to authorised officers further increases this risk (see Case Study 2).

We recommended the department revises its authorisation made under s 5AB of the Act to remove APS Level 6 officers and limits its authorisation instrument to positions that meet the threshold of a management office or management position, which at all other agencies is at least at the EL1 level. At most agencies, authorised officers are at least EL2 level (or equivalent).

The Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment Bill 2007 provided the following guidance about a management office or management position, noting these terms are not defined in the Act:

> *For the purposes of Chapter 4 of the TIA Act (Access to telecommunications data), a management office or management position refers to a role of authority within an enforcement agency to which various management duties and functions are attached, and to which successive people can be appointed… For example… [a] management office or management position in a civilian based enforcement agency such as the Australian Taxation Office*

or the Australian Customs Service would include those employees at the Senior Executive Service (SES) level.

The Department advised the responsibilities of an APS Level 6 authorised officer role is consistent with the Department's organisational structure and official definition of a management role. An APS 6 level officer who supervises other staff is considered by the Gepartment to be in a management position.

We consider this to be an area of significant concern and our Office continues to engage with the department on this issue.

Demonstration of required considerations when deciding whether to authorise disclosure of telecommunications data

Section 180F of the Act requires that authorised officers must, before deciding to make an authorisation disclosing telecommunications data under the Act, 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. Under section 186A(1)(a)(i) of the Act agencies also must keep documents or other materials that indicate an authorisation was properly made including whether all relevant considerations were taken into account.

The Act sets out considerations the authorised officer must consider in weighing up whether the privacy intrusion is justified and proportionate:

- 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 other less intrusive methods were used.

In our 2018–19 report we noted instances at 5 of the 10 agencies inspected where we were unable to assess whether the authorised officer had enough information at the time of making the authorisation to be satisfied that disclosure of the data was justified and proportionate. In the absence of a detailed written request, a contemporaneous record of any verbal briefing provided, or personal considerations of the authorised officer must be made. We did not consider template wording stating the required considerations were made sufficient to demonstrate the required considerations.

Following the 2020–21 inspection period we clarified our position on this issue. We consider template wording to demonstrate authorised officer considerations is sufficient when there is comprehensive and specific information in the request that addresses all relevant considerations under Chapter 4 of the Act (including s 180F of the Act), and it can be demonstrated the authorised officer considered this information in making their decision. Where the request does not sufficiently address all relevant considerations, we look for records to demonstrate what further information the authorised officer turned their mind to in satisfying themselves of these considerations.

We made similar findings about required considerations for 16 of 18 agencies inspected during 2019–20. While many agencies had relatively effective procedures in place, we identified there was insufficient awareness and a lack of training around the requirements of the Act at some agencies, particularly at police forces.

Importance of effective training and guidance for officers exercising telecommunications data powers

It is essential that all officers exercising telecommunications data powers receive and have access to formal training and guidance material to ensure they have a thorough understanding of their obligations under the Act. The absence of formal training and guidance material creates the risk that requests made to authorised officers contain insufficient information and agencies are not adequately supporting authorised officers in their decision-making role. These gaps in awareness can lead to systemic compliance issues.

During our 2019–20 inspections we identified several agencies with insufficient information or an absence of training and guidance material for officers exercising the telecommunications data powers. We further identified that agencies without effective training or guidance material also experienced greater issues in understanding and applying fundamental aspects of the Act including maintaining records demonstrating that authorisations were properly made.

The absence of formal training and practical guidance material also presents a risk to continuity of corporate knowledge. Staff turnover and officers acting in positions as an authorised officer presents a risk of gaps in knowledge and understanding of obligations under the Act. It is essential that formal training and practical guidance is provided to ensure the required knowledge is maintained.

Case study 2 below illustrates how a lack of effective training and guidance material can affect agencies' compliance with the Act.

Case study 2 – New South Wales Police Force, Tasmania Police, Australian Federal Police

During our 2019–20 inspection we identified that several agencies provided insufficient levels of training and support to staff exercising telecommunications data powers under the Act.

Our inspection of the NSW Police Force identified an absence of formal training and written procedures for managing telecommunications data. At the Tasmania Police and the Australian Federal Police we identified that the guidance material was insufficient to support staff to understand their obligations under the Act.

At all 3 agencies we identified instances where authorisations were made without sufficient information included in requests as to why the telecommunications data was to be disclosed. In the absence of a record of personal considerations being made by authorised officers we were not satisfied the authorisations were properly made. Reliance on template wording in these authorisations, where the request did not sufficiently address all relevant information, did not demonstrate the authorised officer had made the required considerations.

We made recommendations and suggestions to these agencies around the need to provide training and guidance to authorised officers on their record-keeping requirements under the Act, and to implement a consistent quality of compliance-focused guidance material and formal training for exercising the powers under Chapter 4 of the Act. All 3 agencies advised our Office they will undertake remedial action and this will be a focus of our future inspections.

Insight into our telecommunications data inspections

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

In some instances carriers may provide additional information that an agency did not specifically authorise. When this occurs we expect an 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 an authorisation. We also undertake our own assessments of the data received by an agency when inspecting the records of authorisations that fall within our sample.

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

- is within the parameters of an authorisation including relating to the correct service number and within the relevant timeframe specified on an authorisation
- is the type of data that was authorised for disclosure by an agency
- does not contain the content of a communication.

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

Example parameters	
Authorised Number	0491 570 006 [16]
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

[16] 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.

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. NB: 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 and not calls received by this number.
10	This line is authorised as after conversion to AEST it occurred at 30/06/2019 1559 being before the time the authorisation was notified to the carrier.
11	This line is not authorised as it is dated after the time the authorisation was notified to the carrier.
For these results it is our expectation that the agency was able to proactively identify and quarantine this data (lines 3 and 11) before results were disseminated to an investigator. Where this unauthorised information is not identified before being sent to investigators, we suggest the agency contact any recipients and quarantine the data. We would also suggest the agency ascertain whether use or disclosure has taken place.	

Findings from telecommunications data inspections conducted in 2019-20

1. Australian Competition and Consumer Commission

We inspected the ACCC from 9 to 12 December 2019 covering records for the period 1 July 2017 to 30 June 2019. We made **5 suggestions** and **3 better practice suggestions** and sent the ACCC a report outlining our findings on 28 April 2020.

Table 41 – Telecommunications data inspection statistics: Australian Competition and Consumer Commission

Telecommunications Data Authorisations			
Records year	**Type of records**	**Records made available**	**Number of records inspected**
2017-18	**Historic**	61	23 (37.5%)
2018-19	**Historic**	108	33 (30.5%)

Progress since previous inspection

During our 2019–20 inspection, we were satisfied that the ACCC has taken appropriate remedial action to address issues identified at our last inspection.

Significant findings

We identified instances where telecommunications data was accessed without proper authority and where data was received outside the period authorised. One of these instances involved the ACCC undertaking multiple 'cascading' searches. The ACCC conducted an Integrated Public Number Database (IPND) search on each service number returned under the original search without those service numbers being authorised. The ACCC advised it quarantined results obtained from this search and amended its processes to ensure cascading searches do not occur.

We also identified the ACCC sets a date range for IPND authorisations to limit the period of results to those relevant to the investigation. While this demonstrates consideration of limiting the privacy intrusion, in practice IPND searches do not permit a date range to be applied. As such, these searches invariably return results outside the period specified on the authorisation. The ACCC advised our Office it updated its processes in line with our suggestions to ensure compliance with the Act.

We also identified an inconsistent approach by investigators when confirming that a request does not relate to a JIW. Despite other processes the ACCC has in place, the inconsistent acknowledgement of these requirements indicated a possible lack of awareness of the JIW provisions. In addition to suggesting the ACCC review its processes relating to JIWs we made a better practice suggestion that it include a more generalised prompt as to whether the request relates to a journalist. The ACCC proactively engaged with our Office on improvements to its processes including providing revised templates for comment.

Table 42 – Telecommunications data inspection findings: Australian Competition and Consumer Commission

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Telecommunications data obtained outside the authorised period				
Unauthorised access to telecommunications data and data outside the parameters of the authorisation	10[17]	-	3 Suggestions	s 180F s 178(2)
Maintaining detailed records where quarantining has taken place	General finding	-	1 Better practice suggestion	-
Journalist Information Warrant procedures				
Inconsistent consideration to application of JIW provisions	General finding	-	1 Suggestion 1 Better practice suggestion	s 180H
Authorised officer considerations				
Amendments to authorisation not endorsed by authorised officer	2	-	1 Suggestion	s 186A(1)(a)(i) s 180F
Record keeping obligations				
Authorisation including identity of authorised officer making the authorisation	General finding	-	1 Better Practice suggestion	s 5AB
Report to the Minister				
Annual report not provided within required timeframe	General finding	-	-	s 186
Form of authorisations				
Day of authorisation not specified	11	-	-	s 183

2. Australian Criminal Intelligence Commission

Our inspection of the ACIC was held from 2 to 5 December 2019 covering records for the period 1 July 2018 to 30 June 2019. We made **5 suggestions** and **one better practice suggestion** and sent the ACIC a report outlining our findings on 22 May 2020.

[17] In 2 instances the criteria used by the ACCC in searches of the IPND did not match what was specified on the authorisation. The searches omitted the middle name of the person when the authorisations specified a full name and omitted components of an address when a full address was stated.

Table 43 – Telecommunications data inspection statistics: Australian Criminal Intelligence Commission

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Number of records inspected**
Historic	6,555	31 (0.47%)
Prospective	1,279	43 (3%)

Progress since previous inspection

While we identified reoccurring instances where telecommunications data was received outside the parameters of the authorisation, many of these instances were disclosed by the ACIC with appropriate remedial action taken.

Significant findings

We identified instances where there was limited information in the background of the request for telecommunications data for the authorised officer to be satisfied of the various considerations. There was also nothing to indicate that authorised officers had turned their mind to case-specific privacy considerations. We suggested the ACIC implement processes to ensure authorised officers consistently demonstrate the required considerations when making a telecommunications data authorisation as required by the Act (s 186A(1)(a)(i)).

The ACIC disclosed an issue where the locations of service numbers that were in contact with the service number subject to the authorisation (known as the 'B' party) were received instead of locations for the service number specified on the authorisation. This may be a carrier issue. Prior to an update to the ACIC's interception platform this issue was not easily identifiable. We will assess the ACIC's progress in managing this issue at our next inspection.

The ACIC disclosed 4 instances where it was unable to verify whether authorisations were made prior to the carrier receiving notification of the authorisations and one instance where a notification of authorisation was sent to the carrier without an authorisation being made.[18] This data was quarantined by the ACIC during the inspection. Similar issues were also identified at our previous inspection and additional measures were put in place that we consider will address the issue in future.

The ACIC also disclosed that an officer who was previously authorised to make telecommunications data authorisations made 4 authorisations despite no longer being covered by the s 5AB authorisation instrument. While this officer was no longer covered due to a position title change it appeared the officer had acted in good faith believing they remained authorised.

[18] No telecommunications data was disclosed by the carrier in this instance.

Table 44 – Telecommunications data inspection findings: Australian Criminal Intelligence Commission

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Telecommunications data accessed without proper authority				
Authorisation made by officer not authorised under s 5AB	-	4	Suggestion	s 5AB(1)
Notification of authorisation without an authorisation in place	-	5		S 183
Authorised officer considerations				
Considerations not demonstrated by authorised officers	General finding	-	Suggestion	s 186A(1)(a)(i) s 180F
Telecommunications data outside parameters of authorisation				
Data outside date range specified on authorisation	1	7	Suggestion	s 178(2) s 180(2)
Service number searched not listed on authorisation	1	4		
Incorrect service number authorised	-	1		
Incorrect search type conducted[19]	-	4		
Telecommunications data received after revocation took effect	2	7		s 180(7)
Unauthorised location data received	General finding		TBD[20]	S 180(2)
Record keeping obligations				
Retaining notifications to carriers	General finding	1	Better practice suggestion	s 186A(1)(a)(iii)
Discrepancies in annual reporting	-	19	Suggestion	s 178
Other findings				
Incorrect provisions used to request evidentiary certificates[21]	2	-	Suggestion	s 185A

3. Australian Commission for Law Enforcement Integrity

Our inspection was held from 22 to 24 July 2019 covering records for the period 1 July 2017 to 30 June 2019. We made **7 suggestions** and **3 better practice suggestions** and sent ACLEI a report outlining our findings on 30 April 2020.

[19] 2 instances occurred due to the carrier undertaking unauthorised searches.
[20] This is an ongoing issue pending further assessments by our Office.
[21] Where an agency seeks such a certification from a carrier it should seek to utilise provisions that are appropriate to the request type, in this instance s 185A of the Act.

Table 45 – Telecommunications data inspection statistics: Australian Commission for Law Enforcement Integrity

Telecommunications Data Authorisations			
Records year	**Type of records**	**Records made available**	**Number of records inspected**
2017-18	**Historic**	389	46 (11.8%)
	Prospective	164	37 (22.6%)
2018-19	**Historic**	384	47 (12.2%)
	Prospective	88	28 (31.8%)

Progress since previous inspection

ACLEI had addressed most issues identified in our previous inspection in 2017–18 , with some exceptions discussed below.

Significant findings

During this inspection we identified several instances where we were unable to determine if the authorised officer considered the relevant privacy considerations when making an authorisation. This was because ACLEI's authorisation templates included generic wording regarding privacy and there was no mechanism such as a comments field to enable authorised officers to record their personal considerations.

In connection with this, we identified 11 instances where requests for telecommunication data did not establish a clear link between the person of interest and the service number or the link between the person of interest and the offence being investigated. This information is relevant to an authorised officer's ability to weigh privacy under s 180F of the Act.

We suggested that ACLEI ensure requests for telecommunications data contain sufficient information and it develops additional guidance for authorised officers where an authorisation relates to more than one service number. We also made better practice suggestions that ACLEI include an area for authorised officers to make comments on its authorisation template and it should limit the number of services on an authorisation.

We also identified ACLEI was not meeting the requirement under s 184(3) the Act to notify the person (generally a carrier) from whom disclosure of data is sought. ACLEI was relying on another agency to perform these administrative steps on its behalf when it made a prospective authorisation. We suggested ACLEI review its processes for notifying carriers of authorisations and to keep records of when a notification of authorisation occurs to satisfy the record keeping requirements of the Act.

Table 46 – Telecommunications data inspection findings: Australian Commission for Law Enforcement Integrity

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Demonstrating privacy considerations				
Demonstrating and recording authorised officer considerations	General finding	-	Suggestion and better practice suggestion	s 180F s 186A(1)(a)(i)
Insufficient information put before authorised officer	11	-		
Authorisations related to multiple service numbers[22]	General finding	-	Suggestion and better practice suggestion	s 180F
Unclear variations and amendments to authorisations	3	-	Suggestion	s 178(3) s 179(3) s 180(4)
Telecommunications data outside parameters of authorisation				
Telecommunications data received after revocation took effect	2	-	-	s 180(7)
Record keeping obligations				
Retention of notifications	General finding	-	Suggestion	s186A(1)(a)(iii)
Use and disclosure of telecommunications data	General finding	-	Suggestion	s 186A(1)(g)
Recording the time an authorisation was made	2		Better practice suggestion	-
Notification sent to multiple carriers under the same authorisation reference	2	1	-	s 186
Form of authorisations				
Authorisations did not meet the requirements of the Determination	General finding	-	Suggestion	s 183
Other findings				
Notification of authorisations and retentions of notifications	General finding	-	Suggestion	s 184(3)

4. Australian Federal Police

Our inspection was held from 9 to 13 September 2019 covering records for the period 1 July 2018 to 30 June 2019. We made **13 suggestions** and **3 better practice suggestions** and reiterated a recommendation from our previous report and sent the AFP a report outlining our findings on 5 August 2020.

[22] In instances where multiple service numbers are listed on a single authorisation there is an increased privacy intrusion that may require additional justification and consideration by the authorised officer.

Table 47 – Telecommunications data inspection statistics: Australian Federal Police

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	17225	65 (0.37%)
Prospective	4711	30 (0.63%)
Foreign historic (s 180A(2) and s 180A(4))	43	18 (41.80%)
Foreign prospective	0	0 (0.00%)

Progress since previous inspection

We have previously made recommendations to the AFP regarding implementing processes to ensure authorised officers consistently document any information relevant to considering and approving a telecommunications data authorisation. During our 2019–20 inspection, we again identified several instances where we were unable to determine if the authorised officer had made the required considerations. We concluded that, while the AFP had taken action to address most of the issues raised at our previous inspection, those measures were not sufficient to address this recommendation.

Significant findings

The AFP has detailed guidance materials requiring authorised officers to make and record relevant considerations before authorising the disclosure of telecommunications data under the Act, but we found the application of this guidance is inconsistent across the AFP. We identified that individual authorised officers do not apply a consistent approach to making authorisations nor do they use common record keeping mechanisms to demonstrate what they considered at the time of making an authorisation.

For example, in some instances available records did not contain sufficient information to identify links between the specific service numbers and the reason/s they were being sought. While we were able to review further information that set out the reasons for the disclosure, the AFP was unable to demonstrate this relevant information was considered by the authorised officer when the authorisations were made.

We restated the recommendation made in our previous report as these inconsistencies and varied processes ultimately limited the AFP's ability to demonstrate the required considerations under the Act were made. The AFP advised our Office that it amended relevant templates and included instruction for authorised officers in the request form on their obligations. Additionally, the AFP told our Office it had introduced a compulsory online training package for requesting officers.

Table 48 – Telecommunications data inspection findings: Australian Federal Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorised officer considerations				
Insufficient demonstration of authorised officer considerations	General finding	-	Reiteration of recommendation from our previous report	s 180F s 186A(1)(a)(i)
Consistent terminology for approval[23]	General finding	-	Better practice suggestion	s 180(2)
Demonstrating thresholds for foreign authorisations – enforcing a foreign law	2	-	2 suggestions	s 180A(2) s 180A(3)
Ambiguous and non-specific requests[24]	2	-	Suggestion	s 178(2)
Amendment to authorisations not endorsed by authorised officer	1	-	2 suggestions	s 180(2) s 180(6)(b)(i) s 183
Telecommunications data outside parameters of authorisation				
Telecommunications data outside parameters of authorisation	2	-	Suggestion	s 178(2) s 180(2)
Record keeping obligations				
Keeping records of notification of an authorisation	General finding	-	Suggestion	s 186A(1)(a)(iii)
Foreign disclosure not recorded in pre-inspection data	1	-	Suggestion	s 180(4) s 186
Form of authorisations				
Form of revocation of an authorisation (legacy issue)	1	-	-	s 183(1)(f)
Inclusion of disclosure statement on foreign authorisations[25]	2	-	3 suggestions	s 180A(2) s 180A(4) s 180E
Listing authorised officer names and positions on authorisation	General finding	-	Better practice suggestion	s 5AB(1) s 183(1)(f)
Other findings				
Foreign authorisations not stating time zone[26]	1	-	Better practice suggestion	s 180A(2)

[23] Due to ambiguity in phrasing used to indicate approval we suggested, as a matter of better practice, the AFP standardise terminology for approval of authorisations under the Act.

[24] We suggested the AFP should ensure authorisations only authorise the disclosure of *specified* information or documents and avoid the use of vague or open-ended language. The AFP advised these occurrences were highlighted as part of its training in this area.

[25] We identified 2 authorisations made under s 180A(2) of the Act which included a statement made under s 180E of the Act. The inclusion of a s 180E statement on the face of an authorisation may give rise to the misapprehension the authorisation also permits the disclosure of information to a Foreign Law Enforcement Agency without a separate authorisation being made. The AFP advised that no information was disclosed to the foreign law enforcement agency.

[26] As the foreign law enforcement agency sets out the parameters for the search, the AFP must clearly indicate which time zone applies to the authorisation to avoid ambiguity about what is authorised. While the carrier did not provide any data outside the terms of the authorisation, this instance highlights the risk of a carrier applying their own interpretation of the parameters if the AFP is not sufficiently clear about what data is authorised for disclosure.

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Use and disclosure provisions to request evidentiary certificates	1	-	2 suggestions	s 185A

5. Australian Securities and Investments Commission

Our inspection of ASIC was held from 21 to 24 October 2019 covering records for the period 1 July 2018 to 30 June 2019. We made **4 suggestions** and **4 better practice suggestions** and sent ASIC a report outlining our findings on 15 April 2020.

Table 49– Telecommunications data inspection statistics: Australian Securities and Investments Commission

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	1,822	40 (2.20%)
Prospective	37	13 (35.14%)

Progress since our previous inspection

At this inspection we were satisfied that ASIC had taken adequate remedial action to the findings set out in our 2018–19 report.[27]

Significant findings

During the inspection, for many authorisations assessed, we found there was limited background information in the form requesting the disclosure of telecommunications data and no contemporaneous records to confirm what information was provided to the authorised officer at the time they made the authorisation. In the absence of such records we were unable to assess whether the authorised officer demonstrated the required considerations. In response to our suggestion, ASIC advised our Office that it was in the process of implementing additional measures to ensure a consistent practice of contemporaneous written records.

We also identified a practice of including multiple searches on a single request form. We raised with ASIC that, where a series of searches is requested and there is limited background information, the authorised officer must be able to demonstrate they made the relevant considerations, including privacy, for each disclosure.

[27] Our 2018–19 annual report incorrectly reported the number of historic authorisation made by ASIC on page 44. The correct figure was included on page 57. The findings also indicate that ASIC notified an incorrect service number in relation to ss 178(2) and 180(2). Only s 178(2) applied to these instances.

Table 50 – Telecommunications data inspection findings: Australian Securities and Investments Commission

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorised officer considerations				
Insufficient demonstration of authorised officer considerations	General finding	-	Suggestion	s 180F s 186A(1)(a)(i)
Telecommunications data outside parameters of authorisation				
Location based searches inconsistent with authorised times	5	-	Better practice suggestion	s 180(2)
Incorrect search parameters due to typographical errors	1	4	Suggestion	s 178(2)
Data outside time specified on authorisation	1	6		s 178(2) s 180(2)
Incomplete search of authorised parameters by carrier	-	1		
Incorrect search parameters entered on authorisations	-	8		
Omission of authorised search parameters on IPND searches	General finding	-	Suggestion	s 178(2) s 179(2)
Record keeping issues				
Unable to assess compliance – results not available[28]	2	-	-	-
Retaining notifications to carriers	-	3	Better practice suggestion	s 186A(1)(a)(iii)
Recording details to indicate when persons are acting in authorised officer position	General finding	-	Better practice suggestion	S 186A(1)(a)(i)
Reporting to Minister				
Authorisations not reported to Minister	3	-	Suggestion	s 186(1)
Form of authorisations				
Meeting the requirements of Communications Access Coordinator Determination (CAC Determination)[29]	4		Better practice suggestion	s 183(1)(f)

6. Corruption and Crime Commission Western Australia

We inspected the CCC WA from 19 to 23 August 2019 covering records for the period 1 July 2017 to 30 June 2019. We made **3 suggestions** and **3 better practice suggestions** and sent the CCC WA a report outlining our findings on 16 July 2020.

[28] This occurred from an IPND search returning a large set of results that were not available to ASIC without making a request to the carrier. We highlighted that consideration be given to limiting certain searches to mitigate against many results being unnecessarily received.

[29] https://www.legislation.gov.au/Details/F2018L01592

Table 51 – Telecommunications data inspection statistics: Crime and Corruption Commission Western Australia

Telecommunications Data Authorisations			
Records year	**Type of records**	**Records made available**	**Number of records inspected**
2017–18	**Historic**	126	42 (33.3%)
	Prospective	99	41 (41.4%)
2018–19	**Historic**	121	41 (33.9%)
	Prospective	63	31 (49.2%)

Progress since our previous inspection

At our previous inspection report we made 2 suggestions to the CCC WA. At this inspection we were satisfied it had taken adequate remedial action in response to these suggestions.

Significant findings

We identified one instance where the request to access telecommunications data did not include relevant information to enable the authorised officer to make all required considerations including the privacy considerations under s 180F of the Act. The service was not subscribed to the person of interest (POI) and there was no clarifying information that set out how the POI was linked to the service. This information is relevant to enable the authorised officer to weigh the privacy considerations.

We considered the CCC WA's ability to demonstrate considerations by authorised officers could be improved through a consistent mechanism to allow authorised officers to record comments, as we identified differing practices in place to achieve this.

We also noted a number of instances where, in an attempt to address the privacy impact of an authorisation, it appeared that requesting officers minimised the potential impact on privacy rather than providing complete information that would assist the authorised officer.

Table 52 – Telecommunications data inspection findings: Corruption and Crime Commission Western Australia

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorised officer considerations				
Insufficient demonstration of authorised officer considerations	1	-	Better practice suggestion	s 180F
Telecommunications data outside parameters of authorisation				
Omission of authorised search parameters on IPND searches [30]	-	11	Suggestion	s 178(2)
Incorrect service number transposed onto authorisation	-	1	-	s 10(1)(g) of the CAC Determination
Record keeping obligations				
Insufficient records to determine compliance with record keeping obligations	2	1	Better practice suggestion	s 186A(1)(a)(i)
Recording the time an authorisation was made	General finding		Better practice suggestion	-
Inconsistent records on when revocation notified to carrier	3	-	Suggestion	s 186(1)(b)(ii)
Form of authorisations				
Authorisation did not include particulars of offence	3	-	Suggestion	s 183(1)(f)

7. Crime and Corruption Commission Queensland

We inspected the CCC QLD from 26 to 29 August 2019 covering records for the period 1 July 2018 to 30 June 2019. We made **4 suggestions** and **3 better practice suggestions** and sent the CCC QLD a report outlining our findings on 19 December 2020.

Table 53 – Telecommunications data inspection statistics: Crime and Corruption Commission Queensland

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	1015	43 (4.24%)
Prospective	225[31]	30 (13.33%)

Progress since previous inspection

At our 2019–20 inspection we were satisfied the CCC QLD had taken adequate remedial action to address our previous findings. However we made further suggestions to encourage improvement in the authorisation process.

[30] In these instances searches of the IPND were conducted where search terms were omitted or broadened which in effect delivered data outside what was authorised.

[31] The actual number of prospective authorisations is lower as revocations of authorisations were also counted as authorisation by the CCC QLD.

Significant findings

At our previous inspection we observed that CCC QLD placed responsibility on requesting officers and other CCC QLD officers in the CCC QLD's internal review process to demonstrate the required considerations under the Act rather than the authorised officer. The CCC QLD's request forms required these officers to make statements addressing the privacy considerations under s 180F of the Act and provided no mechanism for the authorised officer to demonstrate consideration of privacy.

During this inspection we highlighted that template wording or generic statements are not sufficient to demonstrate whether the authorised officer had made the requisite considerations. We identified instances where the information on the request form was insufficient to establish the link between the service subject to an authorisation and the person of interest for the investigation. We suggested the CCC QLD explore and implement measures to consistently demonstrate the required considerations are being made by the authorised officer.

Table 54 – Telecommunications data inspection findings: Corruption and Crime Commission Queensland

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorised officer considerations				
Insufficient demonstration of authorised officer considerations	1	-	Suggestion	s 180F
Insufficient records to link offence to disclosure provision	-	3	Better practice suggestion	s 178(2) s 179(2)
Authorisation in respect of two persons[32]	1	-	-	s 180F
Journalist Information Warrant procedures				
No prompts on templates relating to journalist information warrant requirements	General finding	1	Better practice suggestion	s 180H
Telecommunications data outside parameters of authorisation				
Data received after revocation took effect	3		-	s 180(7)
Record keeping obligations				
Maintaining records of where quarantining of data has occurred	2		Better practice suggestion	-
Not consistently stating authorised officer position or name	25		Suggestion	s 183(1)(f)
Notifications of authorisation not on file	14		Suggestion	186A(1)(a)(iii)
Determining when a revocation takes effect (legacy issue)	General finding	-	-	s 180(7)

[32] This appeared to be an isolated instance. The CCC QLD advised it would update its instructions to reflect that authorisations should only relate to one person.

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Form of authorisations				
Form of authorisations and revocation did not meet requirements of CAC Determination (legacy issue)	General finding	-	-	s 183(1)(f)
Inclusion of s 180(3) on prospective authorisations[33]	General finding	-	-	s 180(3)
Notification of authorisation did not meet form requirements	General finding	-	Suggestion	s 183(1)(f)
Reporting to Minister				
Revocations incorrectly reported as authorisations	3	-	-	s 186(1)(c)

8. Department of Home Affairs

We inspected the Department from 30 September to 4 October 2019 covering records for the period 1 July 2018 to 30 June 2019. We made **3 recommendations**, **20 suggestions** and **3 better practice suggestions** and sent a report outlining our findings to the Department on 20 July 2020.

Table 55 – Telecommunications data inspection statistics: Department of Home Affairs

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	3321	50 (1.51%)
Prospective	225	44 (19.56%)

Progress since previous inspection

We previously identified an issue where the Department received telecommunications data outside the date range specified on the authorisation. While this issue was seen again at our 2019–20 inspection, it has been addressed by the Department's newly introduced telecommunications request portal.

Significant findings

During the inspection we were not satisfied the APS 6 level officers designated as authorised officers at the Department (and who make the bulk of its telecommunications data authorisations) are sufficiently senior to meet the requirements of the Act[34] even where they supervise other staff. As noted above in case study 1 to Part D, the Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment Bill 2007 outlined that a civilian management office or management position would include employees at the Senior Executive Service (SES) level.

[33] Section 180(3) of the Act enables a prospective authorisation to request historic information. Authorisations including this provision is an area of risk as this provision alone is insufficient to request disclosure of historic information without specifying the information to be disclosed. The CCC QLD advised it would maintain separate processes for requesting historic and prospective information.

[34] See Case Study 1 above.

We consider there are significant risks associated with authorised officers designated at an APS 6 level, further heightened when APS 6 positions are temporarily filled by APS 5 officers. Unlike telecommunications interception and stored communications powers under the Act, telecommunications data powers are authorised internally. There is no external issuing authority such as an AAT member or Judge. These decisions can involve significant privacy intrusions, and balancing this intrusion with the usefulness/relevance of the information authorised for disclosure is an important step performed by the authorised officer. More senior officers typically have greater exposure to higher risk and higher responsibility decision-making resulting in a greater appreciation for the gravity of the role and the need to weigh up competing interests such as the potential utility of the information for an investigation, alongside the privacy intrusion access to the information would cause.

Due to risks associated with this practice we recommended the Department revise its s 5AB(1) authorisation under the Act to remove APS Level 6 officers and limit its authorisation instrument under s 5AB(1) to positions that meet the threshold of a management office or management position. The Department did not accept this recommendation. The Department maintained the view that management responsibilities of the authorised APS 6 officers are within the scope of similar departmental APS 6 level management roles exercising delegated statutory powers. We engaged further with the Department on this issue and explained the ongoing risks.

Our concerns were heightened by the lack of approved policies or instructions at the Department relating to telecommunications data under the Act. There was also limited practical guidance on the considerations and obligations required of authorised officers. This lack of awareness of the obligations was reflected in the records inspected where authorisations had limited information to indicate what considerations were made by the authorised officer.

For this reason we recommended the Department implements its policy statement and procedural instructions regarding Chapter 4 of the Act as a priority and ensures these documents provide sufficient guidance on the obligations of authorised officers under Chapter 4. We also recommended the Department makes additional guidance material available specifically to those performing the role of authorised officer and implement training to support decision making and increase awareness of legislative obligations under Chapter 4 of the Act, including the considerations an authorised officer must make in authorising disclosure of telecommunications data. The Department advised the policy statement has been finalised and the procedural instruction is in the final stages of consultation.

In assessing the Department's management of telecommunications data, we were not satisfied that it was able to identify any unauthorised data received and appropriately manage any use and disclosure that may have occurred. The Department did not have a specific policy or written guidance regarding the vetting of telecommunications data nor policies or procedures on use and disclosure of telecommunications data. We consider a consistent approach, guided by policy, is necessary to ensure that data vetting occurs effectively and use and disclosure only occurs in circumstances permitted by the Act.

During the inspection we reviewed an authorisation which related to multiple persons and telecommunications services. However, this authorisation omitted the telecommunications service numbers. This information was recorded on a separate document unconnected to the authorisation and did not appear to have been provided to the authorised officer. Given the absence of a connection to the service numbers we could not determine what was authorised and were not satisfied these authorisations were properly made. No adequate explanation was provided about why the service numbers were not provided to the authorised officer.

Table 56 – Telecommunications data inspection findings: Department of Home Affairs

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorised officers (generally)				
Authorisations made by junior (not Executive Level) officers	General finding	-	Recommendation	s 5AB(1)
Insufficient support, guidance and training	General finding	-	2 recommendations	
No express statement in the s 5AB(1) authorisation instrument regarding acting in a position under delegation	General finding	-	Better practice suggestion	
Demonstration of considerations by authorised officers				
Insufficient demonstration of considerations[35]	General finding	-	Suggestion	s 180F s 186A(1)(a)(i)
Determining what was authorised	General finding	-	2 suggestions	s 186A(1)(a)(i)
Inconsistent authorised periods	2	-		
Inclusion of s 180(3) on prospective authorisations[36]	General finding	-	Suggestion	s 180(2) s 180(3)
Inclusion of multiple requests on an authorisation[37]	General finding	-	Suggestion and better practice suggestion	s 180F
Unclear processes regarding authorisation amendments	5	-	Suggestion	s 186A(1)(a)(i) s 183(1)(f)
Journalist Information Warrant procedures				
Insufficient practical guidance and inbuilt prompts on journalist information provisions	General finding	-	Suggestion and better practice suggestion	s 180H
Management of telecommunications data				
No policy and procedures relating to data vetting and quarantining	General finding	-	3 suggestions	s 178(2) s 179(2)
No policy and procedures to record use and disclosure	General finding	-	2 suggestions	s 186A(1)(g)
Telecommunications data outside parameters of authorisation				
Data outside date range specified on an authorisation	2	2	Suggestion	s 178(2)
Incorrect date range notified to carrier	-	2		
Incorrect service number notified to carrier	-	2		
Data received in relation to incorrect service number	1	-		

[35] The Department's new Telco Request Portal includes fields for authorised officers to make comments on an authorisation. We will review this in practice at future inspections.

[36] This practice was adopted by the Department to cover instances where historic data may be inadvertently returned by a carrier under a prospective authorisation. While a prospective authorisation may specify s 180(3), there was no active demonstration the Department was authorising this information. We were not satisfied that it was appropriate to use this provision to cover such inadvertent instances.

[37] Despite the Department's practice of including multiple services on an authorisation there was no specific policy guidance on ensuring each service requested is considered on its individual merits.

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorisations notified under incorrect legislative provisions[38]	3	-	Suggestion and reiteration of above suggestion (Policy and procedures relating to data vetting and quarantining)	s 183 s 183(1)(f)
Authorisations processed by carrier under incorrect provision	-	2		
Form of authorisations				
No signature on authorisation	-	2	Suggestion	s 183 s 183(1)(f)
Use of additional authorisation/notification documents in relation to carrier records[39]	General finding	-	Suggestion	s 183(1)(f)
Positions of authorised officers not always stated	General finding	-	Suggestion	s 5AB(1) s 183(1)(f)
Record keeping obligations				
Keeping information on the type of authorisations made[40]	General finding	-	Suggestion	s 186A(1)(i)
Recording particulars of the offence to which the authorisation relates[41]	General finding	-		s 110A(1A)
Retention of notifications to carriers	General finding	-	Suggestion	s 186A(1)(a)(iii)
Other issues				
Request sent to incorrect carrier	-	2	-	s 184(3) s 183(1)(f)
Use and disclosure provisions to request evidentiary certificates[42]	General finding	-	suggestion	s 185A

9. New South Wales Crime Commission

We inspected the NSW CC was from 15 to 18 July 2019 covering records for the period 1 July 2017 to 30 June 2019. We made **4 suggestions** and sent NSW CC a report outlining our findings on 7 February 2020.

[38] In these instances the Department notified the carrier that the authorisations were made under s 178(2) of the Act rather than s 179(2).

[39] Where a request for telecommunications data is sent via fax to Telstra, the Department provides a separate notification document signed by the authorised officer. However, we highlighted the potential for ambiguity around which document is in fact the authorisation. We suggested the Department revise its practice where 2 documents purport to be 'authorisations', to remove any ambiguity as to which document is the authorisation and mitigate the risk of discrepancies between the notification and authorisation.

[40] The Department's practices for recording authorisations during the inspection period did not include the specifics of the type of search authorised under a telecommunications data authorisation. Several different searches may be undertaken under Chapter 4 each with varying levels of privacy intrusion. For our Office to identify areas of risk, we require further information on the specific type of search the agency conducted. In response to our report the Department noted it had accepted our suggestion to include additional information in its register of authorisations including the type of authorisations and particulars of offences to demonstrate compliance.

[41] Under s 110A(1A) of the Act the Department, unlike other law enforcement agencies, is only considered a criminal law enforcement agency that can make authorisation under Chapter 4 in relation to offences under five specific Acts. We were not able to assess whether the Department had made authorisations in relation to these five Acts as it did not keep centralised records identifying which Act applied.

[42] While this practice had ceased at the time of the inspection, we suggested the Department review the accuracy of its reporting to the Minister.

Table 57 – Telecommunications data inspection statistics: New South Wales Crime Commission

Telecommunications Data Authorisations			
Records year	**Type of records**	**Records made available**	**Number of records inspected**
2017-18	**Historic**	2893	21 (0.72%)
	Prospective	1149	28 (2.43%)
2018-19	**Historic**	3323	29 (0.87%)
	Prospective	1176	30 (2.55%)

Progress since previous inspection

There were no findings from the previous inspection that required the NSW CC to take action.

Significant findings

The NSW CC advised that verbal authorisations are given by some authorised officers in urgent circumstances. While the NSW CC kept sufficient records around verbal authorisations and the information put before the authorised officers, the Act does not provide for verbal authorisation. We suggested the NSW CC ensure all authorisations are in written or electronic form. The NSW CC informed our Office that it circulated information to all requesting and authorising officers reminding them of the requirement that telecommunications data authorisations must be in written form, and it created templates for written authorisations to be used in urgent circumstances.

Table 58 – Telecommunications data inspection findings: New South Wales Crime Commission

Issue	**Identified**	**Disclosed**	**Suggestion/ Recommendation**	**Section of Act**
Authorised officers (generally)				
Verbal authorisations	General finding	-	Suggestion	s 183
Telecommunications data outside parameters of authorisation				
Data outside date range specified on an authorisation	2	-	3 suggestions	s 180(2)
Data appearing to be outside parameters of authorisation	2	-	-	s 180(2)

10. Independent Commission Against Corruption (New South Wales)

We inspected the ICAC NSW from 10 to 13 March 2020 covering records for the period 1 July 2017 to 30 June 2019. We made **9 suggestions** and **one better practice suggestion** and sent the ICAC a report outlining our findings on 16 July 2020.

Table 59 – Telecommunications data inspection statistics: Independent Commission Against Corruption

Telecommunications Data Authorisations			
Records year	**Type of records**	**Records made available**[43]	**Number of records inspected**
2017-18	**Historic**	298	26 (8.7%)
	Prospective	75	10 (52.6%)
2018-19	**Historic**	291	9 (3.1%)
	Prospective	19	7 (9.3%)

[43] Prospective authorisation figures may not be accurate for the reasons set out in the findings below.

Progress since previous inspection

We were satisfied that the ICAC NSW took sufficient remedial action in response to a small number of issues identified at our previous inspection in 2017.

Significant findings

ICAC NSW did not have a policy or procedures on record keeping obligations for the use and disclosure of Chapter 4 information which led to ICAC NSW not being able to consistently demonstrate compliance regarding use and disclosure requirements and recordkeeping. We suggested the ICAC NSW develop a procedure to clarify the obligations to keep records that indicate whether the use or disclosure of data complied with the Act. The ICAC NSW advised it implemented a 'Use and Communications' register for Chapter 4 requests and has communicated this to Chief Investigators.

While the ICAC NSW undertakes data vetting as a matter of course there was no written guidance on how to vet or manage telecommunications data received from a carrier. We suggested the ICAC NSW document its data vetting process to ensure it is consistently and effectively applied. The ICAC NSW advised it will prepare guidance materials and training regarding data vetting practices.

Table 60 – Telecommunications data inspection findings: Independent Commission Against Corruption New South Wales

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Demonstration of considerations by authorised officers				
Insufficient demonstration of considerations	7	-	Better practice suggestion	s 180F
Journalist information warrant procedures				
Strengthening inbuilt prompts on journalist information provisions	General finding	-	Suggestion	s 180H
Management of telecommunications data				
No policy and procedures relating to data vetting and quarantining	General finding	-	Suggestion	s 178(2) s 179(2) s 180(2)
No procedures to govern use and disclosure obligations	General finding	-	2 suggestions	s 186A(1)(g)
Record-keeping obligations				
Unable to assess compliance – results not available[44]	General finding	-	Suggestion	-
Retention of notifications to carriers	General finding	-	Suggestion	s 186A(1)(a)(iii)
Reporting to Minister				
Discrepancy in figures reported in annual report[45]	6	-	Suggestion	s 186

[44] As the ICAC NSW had deleted, rather than quarantined, unauthorised data received, we were unable to assess the particulars of the non-compliance.

[45] For the 2017–18 period there was a discrepancy in the authorisation data figures reported to our Office as pre-inspection data listed 19 prospective authorisations whereas the ICAC NSW's annual report lists 25. The ICAC later advised that six authorisations had been omitted from the pre-inspection data due to an administrative error.

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Form of authorisations				
Authorised officer position not stated on authorisation	2	-	Suggestion	s 183(1)(f)
Form of authorisation did not meet requirements of CAC Determination	General finding	-	Suggestion	

11. New South Wales Police Force

We inspected the NSW PF from 11 to 14 November 2019 covering records for the period 1 July 2018 to 30 June 2019. We made **9 recommendations, 12 suggestions** and **2 better practice suggestions** and sent the NSW PF a report outlining our findings on 17 September 2020.

Table 61 – Telecommunications data inspection statistics: New South Wales Police Force

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	110,162	39 (0.035%)
Prospective	1,062	41 (3.86%)

Progress since previous inspection

During our previous inspection we identified that one command continued to make verbal authorisations which is not permitted under the Act. We recommended that NSW PF 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. This was identified again during our 2019–20 inspection, discussed below.

Significant findings

Verbal authorisations

NSW PF advised it had implemented our previous recommendation from our November 2019 inspection. However, we again identified the same command continued to make verbal authorisations. As a result we recommended the NSW PF immediately review its authorisation practices and ensures that, prior to requesting the disclosure of any telecommunications data, authorisations are in written or electronic form and signed by the relevant authorised officer in accordance with s 183 of the Act. We also recommended the NSW PF identifies all records where a written authorisation was not in place before telecommunications data was disclosed and quarantine these results until after our 2021–22 inspection, after which time the unauthorised data should be destroyed. The NSW PF should also seek to ascertain whether the unauthorised data has been used or disclosed and where it has, obtain advice about appropriately managing the information.

Retaining required records

We were unable to complete our compliance assessments because NSW PF could not provide our Office with all required records. Records, such as data accessed under certain authorisations, were not made available during the inspection and other required records were only made available on the final day of the inspection. Due to the significant impact this had on our assessments we recommended that NSW PF revises its processes to ensure that all commands and areas are

appropriately meeting their recording-keeping obligations under s 186A of the Act including retaining required records.

We also identified that 583 authorisations reported to our Office by NSW PF predated the 2018–19 inspection period. To ascertain the reasons for this we conducted a spot check of these files and determined that, in some instances, NSW PF relied on a previously actioned authorisations to access telecommunications data in 2019–20. As circumstances change over time, new authorisations should have been made. For example, we identified instances where an authorisation made in 2014, before the revised telecommunications data regime came into effect, was resubmitted to a carrier in 2018 to obtain further updated information with no updated record of privacy considerations made.

This practice circumvented the requirements of s 180F of the Act and the requirements that a disclosure follows a properly made authorisation. We made 2 recommendations for the NSW PF to:

- cease using previously actioned authorisations to request updated data and ensures it makes new authorisations for each disclosure of telecommunications data
- quarantine any telecommunications data received where an authorisation was reused for a subsequent disclosure. After our 2021–22 inspection this unauthorised data should be destroyed. The NSW PF should also limit any further use and disclosure of telecommunications data disclosed under such an authorisation. Where use or disclosure has already occurred the NSW PF should seek advice about how to appropriately manage this information.

The NSW PF advised our Office that its systems had been updated to prevent the re-use of previous authorisations to obtain updated or additional information.

We identified 4 instances where, due to organisational change, 2 purportedly authorised officers were not covered by an authorisation under s 5AB(1) of the Act which meant that telecommunications data obtained under these authorisations was without the proper authority. During the inspection the NSW PF took action to remove the ability of the 2 officers to make further authorisations within the system. Following the inspection NSW PF advised that an audit had identified a further 83 authorisations made by these officers. While these officers were no longer covered by the authorisation instrument, it appeared the officers had acted in good faith believing they were still authorised.

We recommended that NSW PF implements procedures to ensure that authorisations made pursuant to s 5AB(1) of the Act are reviewed following organisational changes and ensures the impact of any change is appropriately communicated to those exercising functions under s 5AB of the Act. We also recommended the NSW PF quarantines all telecommunications data obtained without a valid authorisation and confirms whether any use or disclosure has taken place. If use or disclosure has occurred the NSW PF should obtain advice.

Demonstration of considerations and authorised officer training

There was limited information in the request to support an informed decision by the authorised officer for a high percentage of historic authorisations we inspected. This included information such as the link between the person of interest and the service number or how the requested records would assist the investigation. While such information may be known to the authorised officer, in the absence of records, we were not satisfied the authorised officer had sufficient information in front of them to make the required considerations. We also identified the comments field for authorised officers within the workflow was not routinely used.

NSW PF has a large and dispersed cohort of authorised officers making large numbers of authorisations. Given the scale of this issue, coupled with the lack of adequate training, we had significant concerns around how the authorised officer mechanism was operating. We recommended that NSW PF implements formal training for authorised officers to support their decision-making process and understanding of their obligations under the Act. We also recommended the NSW PF establishes procedures to ensure authorised officers demonstrate the required considerations when authorising access to telecommunications data under Chapter 4 of the Act.

The NSW PF advised our Office it had engaged its education area to develop training for authorised officers.

Table 62 – Telecommunications data inspection findings: New South Wales Police Force

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorised officers (generally)				
Verbal authorisations	General finding	-	2 recommendations	s 183
Insufficient support, guidance and training	General finding	-	Recommendation	s 5AB(1)
Demonstration of considerations by authorised officers				
Insufficient demonstration of considerations	General finding	-	Recommendation	s 180F
General authorisation issue				
Reusing previously actioned authorisations	General finding	-	2 recommendations	s 178 s 178A s 179 s 180F
Telecommunications data accessed without proper authority	General finding	-	2 recommendations	s 5AB(1)
Authorisations seeking foreign providers to preserve telecommunication data[46]	-	2	Suggestion	s 178(2) s 178A(2) s 179(2) s 180(2)
Risk regarding duration a prospective authorisation is in force[47]	General finding	-	Suggestion	s 180(6)
Journalist information warrant procedures				
Insufficient inbuilt prompts on journalist information provisions	General finding	-	2 suggestions	s 180H
Insufficient guidance on journalist information provisions	General finding	-	Suggestion	s 180H

[46] NSW PF disclosed it had given several historic authorisations to international carriers to seek voluntary retention of telecommunications data. It appeared NSW PF had relied on s 178(2) of the Act to request the carrier preserve telecommunications data, despite Chapter 4 of the Act not providing any mechanism to request the preservation of telecommunications data. It was unclear from the available records why the requests were progressed in this manner.
[47] NSW PF's template for prospective authorisations states the duration a prospective authorisation is in force, commencing from the date of carrier connection rather than when it was made (signed) as set out in s 180(6) of the Act. This creates a risk the authorisation could exceed 45 days where the carrier is not notified the same day it is signed.

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Telecommunications data outside parameters of authorisation				
Data outside date range specified on an authorisation	2	-	Suggestion	s 178
Management of telecommunications data				
No procedures to govern use and disclosure obligations	General finding	-	Suggestion	s 186A(1)(g)
Record-keeping obligations				
Retention and availability of records to support oversight	General finding	-	Recommendation	s 186
Retention of notifications to carriers	General finding	-	Suggestion	s 186A(1)(a)(iii)
Unable to assess compliance – results not available[48]	General finding	-	Suggestion	-
Reporting to Minister				
Discrepancy in figures reported in annual report	General finding	-	Suggestion	s 186
Form of authorisations				
Authorised officer position not stated on authorisation	2	-	Suggestion Better practice suggestion	s 183(1)(f)
Form of authorisation did not meet requirements of Determination	5	-	Suggestion	
Ambiguity as to which document was the authorisation	General finding	-	Better practice suggestion	

12. Northern Territory Police

We inspected the NT Police from 8 to 12 July 2019 covering records for the period 1 July 2017 to 30 June 2019. We made **16 suggestions** and sent NT Police a report outlining our findings on 23 June 2020.

Table 63 – Telecommunications data inspection statistics: Northern Territory Police

Telecommunications Data Authorisations			
Records year	**Type of records**	**Records made available**[49]	**Number of records inspected**
2017-18	**Historic**	2150	40 (1.9%)
	Prospective	387	48 (12.4%)
2018-19	**Historic**	1869	45 (2.4%)
	Prospective	271	45 (16.6%)

Progress since previous inspection

We are satisfied the NT Police had taken appropriate remedial action on all but 3 of the issues identified at our previous inspection (addressed below).

[48] NSW PF did not have a consistent mechanism to retain location-based results. There were also 5 instances where results were either incomplete or unavailable and one instance where results had been deleted. We were unable to determine whether the telecommunications data the NSW PF had received complied with the parameters of these authorisations.

[49] These figures may not be accurate for the reasons outlined in the findings below.

Significant findings

We identified the NT Police had used a request-based approach to calculating the number of authorisations it made despite a request potentially including multiple authorisations. This resulted in underreporting of the number of authorisations made to the Minister. We also identified general inconsistencies in NT Police's reporting on its use of these powers, for example when we compared its annual report figures with data available to our Office. The NT Police advised the Department had approved provision of an addendum to its 2019–20 annual report with the updated figures from the previous period.

We identified 14 authorisation records where the justification recorded by the authorised officer did not directly address the privacy considerations, made privacy considerations that were inadequate, or addressed considerations other than those required by the Act. For that reason we considered that increased understanding of these requirements across NT Police will also assist requesting officers in supplying sufficient information to support authorised officers' decision-making.

We also identified concerns with the integrity of the authorisation process as we were advised that sometimes officers processing the authorisations will amend an authorisation after it had been made by an authorised officer. While this usually occurred to correct errors, any amendment to the authorisation requires the authorised officer's approval, which did not occur in these instances. Some changes could mean the authorised officer needs to reconsider the privacy implications.

We also identified that NT Police had processed a range of different requests against a category referred to as 'Telecommunications Other'. These requests purported to be made under or were recorded as authorisations under Chapter 4 of the Act. In reviewing records under this category we identified several requests that are precluded from being authorised under Chapter 4 of the Act, specifically s 172 of the Act which prohibits the disclosure of the content or substance of a communication. For example, requests seeking the content of messages and possible access to closed-circuit television (CCTV) footage.

We also identified 2 requests seeking the preservation of data held by a foreign provider which were purportedly authorised using the process for a historic telecommunications data request. Chapter 4 of the Act does not provide a mechanism for preserving telecommunications data and it was unclear from available records why these requests were progressed through the telecommunications data approval workflow. No authorisations were subsequently made in these instances.

NT Police advised policy changes have been implemented to address and prevent non-compliance.

Table 64 – Telecommunications data inspection findings: Northern Territory Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Demonstration of considerations by authorised officers				
Insufficient demonstration of considerations	General finding	-	Suggestion	s 180F
Amendment to authorisation without authorised officer approval (integrity of authorisation process)	General finding	-	2 suggestions	s 180F s 186A(1)(a)(i)
General authorisation issue				

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorisation for content or data not permitted by the Act	2	-	3 suggestions	s 172 s 178(2) s 180F s 186A(1)(a)(i)
Authorisations issued for data preservation	2	-		
Prospective authorisations do not state the specific information to be disclosed[50]	General finding	-	Suggestion	s 180(2) s 183(1)(f)
Content disclosed by carrier under prospective authorisation[51]	-	1	-	s 172
Telecommunications data outside parameters of authorisation				
Data outside date range specified on an authorisation	6	-	2 suggestions	s 178(2)
IPND searches did not match authorised search terms	2	-		
Management of telecommunications data				
Insufficient procedures for vetting telecommunications data	General finding	-	Suggestion	s 178(2) s 178A(2) s 179(2)
Reporting to Minister				
Inconsistent recording and reporting of authorisations made	General finding	-	2 suggestions	
Journalist information warrant procedures				
Insufficient inbuilt prompts on journalist information provisions	General finding	-	Suggestion	s 180H
Insufficient guidance on journalist information provisions	General finding	-	Suggestion	
Record-keeping obligations				
Notification of an authorisation not retained	3	-	Suggestion	s 186A(1)(a)(iii)
Form of authorisations				
Form of notifications did not meet the requirements of the CAC Determination	General finding	-	Suggestion	s 183(1)(f)
Form of historic and prospective authorisations did not meet requirements of the CAC Determination	General finding	-		

[50] Prospective authorisations did not state the specific information to be disclosed but rather only specified 'prospective information'. NT Police's practice is for the specific information requested to be included on a separate notification coversheet when the authorisation is notified to the carrier. While this is an accepted practice at NT Police, we consider that it may create ambiguity as to what an authorised officer has authorised for disclosure and may impact an authorised officer's ability to make the requisite considerations under the Act.

[51] This authorisation was incorrectly provisioned by the carrier as a telecommunications interception. During the inspection we witnessed the destruction of 375 incorrectly received sessions. NT Police advised that change to its platform was made to prevent the processing of any incorrectly provisioned authorisations.

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Person from whom disclosure was sought incorrectly stated	9	-		
Legacy issue: Revocation of prospective authorisations did not meet requirements of Determination	22	-		

13. Queensland Police Service

We inspected the QPS from 20 to 24 January 2020 covering data from the period 1 July 2018 to 30 June 2019. We made **12 suggestions** and **8 better practice suggestions** and sent the QPS a report outlining our findings on 19 June 2020.

Table 65 – Telecommunications data inspection statistics: Queensland Police Service

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Records inspected**
Historic	23,895	62 (0.26%)
Prospective	4252	61 (1.4%)

Progress since previous inspection

At our previous inspection we made 12 suggestions and 8 better practice suggestions. During this inspection we were satisfied that QPS had taken appropriate remedial action for most of the issues raised in our last report.

Significant findings

We identified several issues with authorised officers at QPS not demonstrating considerations in accessing telecommunications data. This limits our ability to be satisfied that authorised officers had the required information at the time the authorisation was made. For one area of QPS there was no background information on request forms and no record of considerations made by the authorised officer. We were unable to be satisfied the required considerations were made for all authorisations by that area. For another area of QPS we identified 3 authorisations where requests did not contain sufficient detail and authorised officers had not recorded their considerations.

To consistently demonstrate compliance with the Act we suggested the QPS implement measures to demonstrate that an authorised officer made the required considerations when authorising a request. QPS acknowledged our suggestion and advised it is developing an instruction on the retention of written records.

We also identified that QPS has no specific compliance-focused training for investigators and authorised officers on using the powers under Chapter 4 of the Act and we considered the awareness among investigators of their obligations under the Act was low. The guidance material used by authorised officers and investigators also lacked practical guidance regarding data vetting, managing use and disclosure and appropriate uses of data.

Table 66 – Telecommunications data inspection findings: Queensland Police Service

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Telecommunications data accessed without proper authority				
Incorrect enabling legislation[52]	2	-	Suggestion	s 178(2) s 179(2)
General authorisation issues				
Content disclosed by carrier under prospective authorisation[53]	-	1	-	s 172
Incorrect service number provided by investigator on authorisation	8	-	2 better practice suggestions	
Telecommunications data outside parameters of authorisation				
Telecommunications data outside date range listed on authorisation	9	-	Better practice suggestion	s 178(2)
Incorrect service number notified to carrier	3	-	Better practice suggestion	s 178(2) s 180(2) s 180F
Demonstration of considerations by authorised officers				
Insufficient demonstration of considerations by authorised officers	8	-	2 suggestions	s 180F s 186A(1)(a)(i)
Management of telecommunications data				
Insufficient procedures for vetting telecommunications data	General finding	-	Suggestion	-
No mechanism for effective quarantining of telecommunications data	General finding	-	Suggestion	s 178
Insufficient governance on use and disclosure of information obtained under historic authorisations	General finding	-	Suggestion	s 186A(1)(g)
Ineffective procedures for recording when	General finding	-	Suggestion	-

[52] In these instances QPS made 2 authorisations under s 179 of the Act, rather than s 178 of the Act.

[53] This authorisation was incorrectly provisioned by the carrier as a telecommunications interception. While incorrectly provisioned, system settings at QPS did not allow any ingested content to be processed.

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
compliance issues occurred				
Insufficient quality assurance measures	9	8	2 suggestions Better practice suggestion	
Journalist information warrant procedures				
Insufficient guidance on journalist information provisions	General finding	-	Better practice suggestion	s 180H
Insufficient inbuilt prompts on journalist information provisions	General finding	-		
Reporting to Minister				
Incorrect reporting of authorisations	2	1	Suggestion	s 186
Record-keeping obligations				
Inconsistent practices to retain notification of an authorisation	General	-	Suggestion	s 186A(1(a)(iii)
Authorisations not fully disconnected by carrier / Unable to confirm information not received after revocation[54]	-	1	-	s 180(7)
Notification to carriers				
Incorrect carrier notified	-	1	Suggestion	s 184(3)
Form of authorisations				
Person from whom disclosure sought not listed	-	1	Better practice suggestion	s 183(1)(f)

14. Independent Commissioner Against Corruption (South Australia)

We inspected the ICAC SA from 24 to 27 February 2020 covering records from the period 1 July 2017 to 30 June 2019. We made **10 suggestions** and **8 better practice suggestions** and sent the ICAC a report outlining our findings on 4 June 2020.

[54] In this instance the carrier had not disconnected the location component of the prospective authorisation. Due to a previous issue with the retention of this dataset at QPS we were unable to assess whether this data had been received.

Table 67 – Telecommunications data inspection statistics: Independent Commissioner Against Corruption (South Australia)

Telecommunications Data Authorisations			
Records year	**Type of records**	**Records made available**	**Number of records inspected**
2017-18	**Historic**	288	65 (12.8%)
	Prospective	220	
2018-19	**Historic**	28	28 (50%)
	Prospective	28	

Progress since previous inspection

In our previous inspection report we made one suggestion to ICAC SA and were satisfied that the ICAC SA had taken adequate action on the issues identified.

Significant findings

We identified the ICAC SA's authorisation process did not have a mechanism to enable or prompt authorised officers to record their considerations. While ICAC SA uses detailed memoranda to support requests for telecommunications data, we did identify omissions in background information relating to why particular records periods were sought without there being personal considerations made by the authorised officer. There was also an instance where a service subject to the authorisation was not subscribed to the person of interest without clarifying information to set out how these 2 were connected. This limited our ability to be satisfied the required considerations were demonstrated.

During our inspection the ICAC SA disclosed, and we identified, several issues relating to Integrated Public Number Database (IPND) searches (which can be made following a historic telecommunications data authorisation), such as variations to addresses on IPND searches, use of date ranges on IPND searches and consistency of wording on IPND authorisations.

IPND system limitations may prevent an agency from applying certain parameters such as date ranges when conducting a search. However, we consider that searches should be conducted strictly in accordance with an authorisation. This prevents any ambiguity as to whether a search was permitted by an authorisation.

Table 68 – Telecommunications data inspection findings: Independent Commissioner Against Corruption (South Australia)

Issue	**Identified**	**Disclosed**	**Suggestion/ Recommendation**	**Section of Act**
Telecommunications data accessed without proper authority				
Authorised officer not correctly stated on authorisation[55]	1	2	Suggestion	s 183
Authorisation not signed – telecommunications data obtained	-	1	-	s 180(2)

[55] In this instance the applicant was listed as the authorised officer which led to ambiguity as to who was purporting to make the authorisation.

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Demonstration of considerations by authorised officers				
Insufficient demonstration of considerations by authorised officers	General finding	-	Suggestion Better practice suggestion	s 186A(1)(a)(i)
No information to link person of interest to service	1	-	Suggestion	s 186A(1)(a)(i) s 180F
Ambiguity of period authorised for disclosure	2	-	Better practice suggestion	180F
Reason for period requested not addressed	General finding	-		
Inconsistencies in date ranges	General finding	-		
Telecommunications data outside parameters of authorisation				
Incorrect service number searched in IPND	2	-	2 suggestions	s 178(2)
Variation to address search in IPND	8	-	Suggestion	
Use of date ranges on IPND searches[56]	General finding	-		
Telecommunications data of a type not authorised received	4	-	Better practice suggestion	
Journalist information warrant procedures				
Insufficient inbuilt prompts on journalist information provisions	General finding	-	Suggestion	s 180H
Management of telecommunications data				
No telecommunications data vetting guidance	-	General finding	Suggestion Better practice suggestion	s 178(2) s 180(2)
No framework for recording use and disclosure	General finding	-	Suggestion	s 186A(1)(g)
Reporting to the Minister				
Authorisation may not have been reflected in annual reporting	-	1	Suggestion	s 186
Record-keeping obligations				
Notification of authorisation not retained	General finding	-	Better practice suggestion	s 186A(1)(a)(iii)
Unable to assess compliance – results not available [57]	-	6	-	-
Inconsistent recording of time an authorisation was made	General finding	-	Better practice suggestion	-
Other issues				

[56] The IPND does not permit a date range parameter to be applied to historical searches. Due to this limitation these searches will invariably return results outside the period specified on the authorisation. The ICAC SA's inclusion of this timeframe was to meet the Department of Home Affairs' reporting requirements on the retention period requested under an authorisation.

[57] In these instances the ICAC SA's searches of the IPND returned too many results and the ICAC SA was not able to access the data. We were therefore unable to assess whether the searches were conducted in accordance with the authorisation.

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Consistency of wording on IPND authorisations	General finding	-	Better practice suggestion	s 180F
No explicit statement on s 5AB authorisation regarding persons acting in positions	General finding	-	Better practice suggestion	s 5AB(1)
Authorisation not reported to our office[58]	1	-	-	186B

15. South Australia Police

We inspected SA Police from 2 to 6 September 2019 covering records from the period 1 July 2017 to 30 June 2019. We made **12 suggestions** and **3 better practice suggestions** and sent SA Police a report outlining our findings on 21 September 2020.

Table 69 – Telecommunications data inspection statistics: South Australia Police

Telecommunications Data Authorisations			
Records year	**Type of records**	**Records made available**	**Number of records inspected**
2017–18	**Historic**	3830 / 5793[59]	61 (1.6% / 1%)
	Prospective	341	53 (15.5%)
2018–19	**Historic**	5836	61 (1%)
	Prospective	422	54 (12.8%)

Progress since previous inspection

In our previous inspection report we made 2 suggestions to SA Police. At this inspection we were satisfied that SA Police had taken adequate remedial action in response to our findings and suggestions.

Significant findings

We identified 3 instances where historic authorisations were purportedly made by an officer who was not covered by the s 5AB(1) authorisation. In one of those 3 instances we considered that insufficient training was a contributing factor. We also identified one instance where disclosure of telecommunications data occurred without there being an authorisation formally made (signed) by the authorised officer.

We identified one instance where an authorisation was given verbally. While a written record of the authorisation was made the same day, the Act requires that authorisations must be signed by their maker and in either written or electronic form. We suggested that SA Police ensures all authorisations are in written or electronic form as required by s 183 of the Act and that it quarantine any telecommunications data obtained without a written authorisation in place at the time of the request.

SA Police advised it had ceased the practice of giving verbal authorisations and had implemented a new process to give approval by email with an authorisation instrument signed at the same time as a record of the decision.

[58] No disclosure occurred under this authorisation as it was never provided to the carrier; however, our Office requires that an agency report all authorisations it has made as part of our inspections.
[59] These figures may not be accurate for the reasons outlined below.

We identified several issues relating to how SA Police kept records demonstrating an authorisation was properly made as required by s 186A(1)(a)(i) of the Act. These issues were a result of insufficient detail to substantiate requests for telecommunications data. In other instances these were the result of certain processes and practices at SA Police that limited or affected its ability to demonstrate compliance.

We identified issues covering the following:

- insufficient information to satisfy us the privacy considerations were made
- no demonstration of the privacy considerations supporting subscriber checks
- multiple authorisations arising from one request that did not include any further records to indicate the need for additional requests or a demonstration of the increased privacy considerations by the authorised officer
- different signatures on authorisation records where the original authorisation request was signed by one authorised officer and the notification and authorisation sent to the carrier were signed by a different authorised officer
- authorisation amendments without clear approval by the authorised officer.

We suggested that SA Police implement processes to enable it to consistently demonstrate that an authorised officer made the required considerations when making an authorisation. We also suggested that SA Police ensure any amendments to authorisations are approved by the originating authorised officer, and appropriately documented.

Table 70 – Telecommunications data inspection findings: South Australia Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Telecommunications data accessed without proper authority				
Authorisations made by an officer who was not an authorised officer	3	-	3 suggestions	s 5AB(1)
Disclosure of telecommunications data without properly made authorisation	1	-		s 183(1)(f)
Verbally approved disclosure	1	-	Suggestion	s 183(1)(e)
Demonstration of considerations by authorised officers				
Insufficient information to be satisfied privacy considerations were made	5	-	2 suggestions 2 better practice suggestions	s 186A(1)(a)(i)
Insufficient demonstration of reason for subscriber checks supporting prospective authorisations	5	-		
Multiple authorisations arising from single request	2	-		s 180F

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Authorisation amended without clear approval by authorised officer	1	-		s 183(1)(f)
Authorisations not linked to considerations[60]	4	-		s 186A(1)(a)
High volume of service numbers listed on authorisation affecting privacy considerations	General finding	-		s 180F s 186A(1)(a)
Telecommunications data outside parameters of authorisation				
Telecommunications data outside date range on authorisation	2	-	2 suggestions	s 180(6)
Telecommunications data received after the time a revocation took effect	1	-		
Form of authorisations				
Basis on which officer is authorised not stated/authorised officer not clearly identified	General finding	-	Suggestion	s 183(1)(f)
Authorisation and revocation templates do not meet prescribed form	General finding	-	Suggestion	
Record-keeping obligations				
Unable to assess compliance – results not available	2	-	-	s 186A(1)(g)
Inconsistent recording of authorisations made	General finding	-	2 suggestions	s 186(1)
Other matters				
Section 5AB authorisation instrument did not reflect organisation structure	General finding	-	Better practice suggestion	s 5AB(1)

16. Tasmania Police

We inspected Tas Police from 25 to 29 November 2019 covering records from the period 1 July 2018 to 30 June 2019. We made **4 recommendations** about Tas Police's overall approach to compliance (as discussed in Part B of this report). We made **3 recommendations** and **13 suggestions** about Tas Police's compliance with Chapter 4 of the Act and sent Tas Police a report outlining our findings on 22 December 2020.

[60] The application supporting these authorisations was signed by an officer other than the authorised officer which meant it was ambiguous who was the approving authorised officer and whether that person had regard to the relevant privacy considerations.

Table 71 – Telecommunications data inspection statistics: Tasmania Police

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Number of records inspected**
Historic	5979	29 (0.5%)
Prospective	185	41 (22%)

Progress since previous inspection

We previously made 2 recommendations, 10 suggestions and one better practice suggestion regarding Tas Police's compliance with Chapter 4 of the Act. While Tas Police had acted on some of our previous findings, it had not adequately addressed other issues.

Significant findings

Demonstration of considerations

While Tas Police adopted a decentralised approval process because of our recommendations, our inspection found that further progress was required to demonstrate that authorised officers were having regard to the required considerations under the Act.

For all historic and prospective authorisations inspected, we did not observe any record of personal considerations made by authorised officers and in many cases the request was inadequate. We identified a lack of information to explain why a disclosure of telecommunications data was reasonably necessary. This was likely because the officer did not possess sufficient understanding of relevant legislative obligations when applying for authorisations. We recommended that Tas Police provide training and guidance to authorised officers on their record-keeping requirements under the Act and implement measures to consistently document any information relevant to their consideration and approval of a telecommunications data authorisation under Chapter 4 of the Act, to demonstrate they took into account all relevant matters. Tas Police informed our Office it has provided guidance to authorised officers in relation to these recommendations.

Training and guidance on managing authorisations

In October 2019 Tas Police introduced a new system for submitting and approving requests for historic telecommunications data authorisations. Based on the information available to our Office and discussions with relevant staff, training that accompanied the commencement of the new system did not include training on processing requests and authorisations under the Act. At the time of our inspection there was not a consistent procedure in place for submitting requests and processing authorisations. Users were either able to subvert the workflow or input information in a manner that was inconsistent with the intended process. Within this new system we identified a lack of critical controls that posed a risk to Tas Police's ability to achieve compliance including:

- no prompting on the type of information a requesting officer should supply to substantiate a request
- no controls regarding journalist information warrant requirements
- no information to make it clear which legislative provisions the requesting officer is relying on to access telecommunications data.

Due to the serious nature of these systems issues and the lack of training available to requesting officers we recommended that Tas Police provide training and establish procedures and guidelines

for submitting authorisations on the new system to ensure it meets its legislative obligations under the Act. We also made 3 suggestions to address the omission of the critical controls highlighted above.

In migrating records into the new system it did not appear that Tas Police considered the impact the changes would have on our oversight and its record keeping obligations under s 186A of the Act. During our inspection Tas Police advised the old system had been decommissioned and this resulted in issues for our Office in assessing compliance with the Act due to difficulties in identifying the authorised officer, when an authorisation was made and the scope and purpose of authorisations processed through the old system.

We recommended that in making any changes to systems, Tas Police actively considers the impact any system change will have on its ability to demonstrate compliance with and meeting its recordkeeping obligations under s 186A of the Act.

As a result of our previous inspection we also made 6 suggestions to Tas Police about quarantining telecommunications data outside the parameters of an authorisation, telecommunications data that was not obtained for a permitted purpose and telecommunications data without valid authorisations. At the time of this inspection Tas Police had not quarantined any data received under the affected authorisations.

Tas Police responded to our inspection report advising it was creating online training and guidance materials to assist staff in confidently navigating requirements of the Act.

Table 72 – Telecommunications data inspection findings: Tasmania Police

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
Demonstration of considerations by authorised officers				
Insufficient demonstration / no mechanism for demonstration of considerations by authorised officers	General finding	-	Recommendation 2 suggestions	s 180F s 186A(1)(a)(i)
Insufficient information on why an authorisation is reasonably necessary	General finding	-	Suggestion	
Authorisations not linked to considerations[61]	6	-	-	
Insufficient prompts on information required to enable considerations to be made	General finding	-	Suggestion	
General authorisation issues				
No training and procedures to support compliant use of new system	General finding	-	Recommendation	-
Insufficient information to highlight legislative obligations	General finding	-	Suggestion	-
Journalist information warrant controls				
Insufficient prompting regarding the journalist	General finding	-	Suggestion	s 180H

[61] We noted a legacy practice where we were not satisfied the authorised officer who made the prospective authorisation had regard to the information on the application when considering whether to authorise the disclosure. This is because the application was signed by a different authorised officer (who had regard to the information in the application) to the authorised officer who signed the authorisation.

Issue	Identified	Disclosed	Suggestion/ Recommendation	Section of Act
information warrant requirements				
Management of telecommunications data				
Insufficient formalised guidance on data vetting for historic and prospective authorisations	General finding	-	3 suggestions	s 178(2) s 178A s 179 s 180(2)
No consistent procedures on compliance with use and disclosure obligations	General finding	-	Suggestion	s 186A(1)(g)
No remedial actions to quarantine unauthorised data highlighted in previous inspection	General finding	-	-	s 178(2) s 178A s 179 s 180(2)
Telecommunications data outside parameters of authorisation				
Telecommunications data unrelated to authorised number received	1	-	Suggestion	s 180(2)
IPND search did not comply with authorised parameters	1	-	Suggestion	s 178(2)
Record-keeping obligations				
Keeping records to indicate whether authorisation were properly made	General finding	-	Recommendation	s 186A(1)(a)(i)
Form of authorisations				
Notifications of IPND do not specify correct authorised officer	General finding	-	Suggestion	s 183(1)(f)

17. Victoria Police

We inspected Vic Police from 28 to 31 January 2020 covering records from the period 1 July 2018 to 30 June 2019. We made **10 suggestions** and **2 better practice suggestions** and sent Vic Police a report outlining our findings on 16 July 2020.

Table 73 – Telecommunications data inspection statistics: Victoria Police

Telecommunications Data Authorisations		
Type of records	**Records made available[62]**	**Number of records inspected**
Historic	93,893	57 (0.06%)
Prospective	11,898	54 (0.45%)

[62] The actual number of authorisations are likely to be lower than reported as some requests for telecommunications data that were rejected and requests for evidentiary certificates appear to have been counted as authorisations.

Progress since previous inspection

At our previous inspection we made 3 recommendations and 5 suggestions to Vic Police. While Vic Police has taken steps to improve its processes and practices, there were still several issues that Vic Police needed to address to meet its compliance obligations.

Significant findings

While there was improvement to the level of background information supporting authorisation requests[63] we identified several instances where sufficient information was not supplied to enable an authorised officer to make the required considerations when approving authorisations made through the request management system.

We identified shortcomings in how authorised officers documented their considerations including instances where there was:

- no documenting of considerations
- inconsistent practices in how considerations were documented
- inconsistencies in the level of detail documented.

Where active considerations are not documented by an authorised officer and the background information in the request is not adequately detailed, we cannot be satisfied an authorised officer made the required considerations. We suggested Vic Police provide training and guidance to authorised officers on their record-keeping requirements under the Act and implement measures to consistently demonstrate an authorised officer made the required considerations when making an authorisation. As a matter of better practice, we also advised Vic Police to incorporate a comments field for authorised officers to include comments demonstrating considerations made and information considered when making an authorisation.

We also suggested that Vic Police ensure requesting officers are made aware of the requirements of the Act, including the information that will enable an authorised officer to appropriately consider a request for telecommunications data in line with Chapter 4 of the Act.

We also suggested that Vic Police ensure it has a consistent framework for identifying and managing telecommunications data received outside the parameters of an authorisation. This suggestion was directed at ensuring all areas of Vic Police conduct data vetting to the same standard to identify unauthorised telecommunications data. We highlighted to Vic Police, that as the area responsible for the majority of telecommunications data authorisations does not undertake centralised vetting (the onus is on investigators to assess whether telecommunications data complies with the parameters of an authorisation), it is essential there is clear and effective guidance in place. We continue to consider this an area of risk.

[63] Following the 2018–19 inspection Vic Police finalised an internal audit to monitor the implementation of recommendations and suggestions from external audits (including our Office) in November 2019. As an outcome, Vic Police communicated with authorised officers about information to be included in requests for telecommunications data made via RMS. Any changes arising from these actions would not be reflected during the 2019–20 inspection due to the retrospective nature of our inspections.

Table 74 – Telecommunications data inspection findings: Victoria Police

Issue	Identified	Disclosed	Suggestion / Recommendation	Section of Act
Demonstration of considerations by authorised officers				
Insufficient background information to enable making of considerations	General finding	-	Suggestion	s 180F s 186A(1)(a)(i) s 180(7)
No active demonstration of considerations by authorised officers	General finding	-	Suggestion Better practice suggestion	
General authorisation issues				
Insufficient awareness of obligations by requesting officers when applying for authorisations	General finding	-	Suggestion	s 186A(1)(a)(i)
Guidance on obligation to revoke authorisations	General finding	-	Suggestion	s 180(7)
Missing person authorisations processed under incorrect provision[64]	General finding	-	-	s 178(2) s 178A(2) s 179(2) s 180(2)
Use of disclosure provisions to request evidentiary certificates	General finding		2 suggestions	s 185A
Management of telecommunications data				
No consistent framework to support accurate data vetting	General finding	-	Suggestion	s 178(2) s 178A(2) s 179(2)
Further measures required to maintain awareness of use and disclosure obligations	General finding	-	Suggestion	s 186A(1)(g)
Journalist information warrant procedures				
Lack of awareness by requesting officers of JIW provisions	General finding	-	Suggestion Better practice suggestion	s 180H
General authorisation issues				
Content disclosed by carrier under prospective authorisation not identified	1	-	-	s 172
Record-keeping obligations				
Notification of authorisation not retained	1	-	-	s 186A(1)(a)(iii)
Unable to assess compliance – results not available	2	-	-	s 186A(1)(a)
Reporting to the Minister				
Over-reporting: rejected authorisations reported to Minister as authorisations made	General finding	-	Suggestion	s 186

[64] Authorisations in relation to missing persons under s 178A were incorrectly processed through RMS under ss 178 or 180. This was a known system issue with RMS and using ss 178 or 180 was a workaround to progress authorisations within the system. In these instances the requesting officer articulated that the request related to a missing person (and would be made by the authorised officer on this basis). An authorisation should only be made under the provision that aligns with the purpose for which it was made as this forms part of the record of an authorised officer's decision-making under s 186A(1)(a)(i) of the Act.

18. Western Australia Police

We inspected WA Police held from 5 to 9 August 2019 covering records from the period 1 July 2018 to 30 June 2019. We made **5 suggestions** and **1 better practice suggestion** and sent WA Police a report outlining our findings on 21 May 2020.

Table 75 – Telecommunications data inspection statistics: Western Australia Police

Telecommunications Data Authorisations		
Type of records	**Records made available**	**Number of records inspected**
Historic	23,397	54 (0.23%)
Prospective	2,117	42 (2.0%)

Progress since previous inspection

At our previous inspection we made 5 suggestions to WA Police. At this inspection we were satisfied that WA Police had taken adequate action in response to our findings and suggestions.

Significant findings

We identified several issues around authorised officer considerations and record keeping including inconsistent practices surrounding subscriber checks. Where WA Police requested a subscriber check for court purposes it had not used a telecommunications data authorisation request form to record any relevant background information as it did for other authorisations. For this reason we suggested that WA Police implement processes to demonstrate the considerations made by an authorised officer for subscriber checks in line with the requirements of s 186A(1)(a)(i) of the Act.

Table 76 – Telecommunications data inspection findings: Western Australia Police

Issue	**Identified**	**Disclosed**	**Suggestion/ Recommendation**	**Section of Act**
Demonstration of considerations by authorised officers				
Authorised officer considerations and record keeping	General finding		Suggestion	s 180F s186A (1)(a)(i)
Process for recording IPND authorisations	General finding		-	s 186
Telecommunications data accessed without proper authority				
No signed authorisation in place prior to IPND search	1	-	Suggestion	s 183
Telecommunications data outside parameters of authorisation				
Telecommunications data received after revocation	2	-	Suggestion	s 180(7)
General authorisation issues				
Use and disclosure to request evidentiary certificates	General finding	-	2 suggestions	s 185A
Recording time an authorisation was made	General finding	-	Better practice suggestion	s 183(1)(e)

Appendix A – Stored communications inspection criteria 2019–20

Audit Objective: To determine the extent of compliance with Chapter 3 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) 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 effective procedures in place to ensure that warrants are properly applied for and issued in the prescribed form (s 118(1))?

Records checks in the following areas:

- Whether applications for stored communications warrants were made in accordance with ss 110 to 113, or ss 111 to 114 and 120(2) for telephone applications
- 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 accordance with s 119(5)
- 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 effective 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

1.3 Did the agency screen stored communications and quarantine any that were unlawfully accessed?

Process checks:

- Does the agency have effective procedures in place to identify and quarantine accessed stored communications that are not authorised by the warrant?

Records checks in the following areas:

- Whether accessed stored communications were within the parameters of the warrant, including any conditions and restrictions (s 117)
- Whether stored communications provided to the agency had been accessed by the carrier(s) while the warrant was in force (s 119)
- Whether the agency identified stored communications that did not appear to have been lawfully accessed, and if appropriate, sought clarification from the carrier(s) and quarantined them from use (s 108)

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 effective procedures and authorisations in place to properly receive accessed stored communications in the first instance?
- Does the agency have secure storage facilities for accessed information?

Records checks in the following areas:

- Whether stored communications were received in accordance with s 135

2.2 Were stored communications properly dealt with and destroyed?

Process checks:

- Does the agency have procedures in place for destroying stored communications and reporting destruction activities?
- Does the agency have controls, guidance and/or training in place to ensure that stored communications are only dealt with for a permitted purpose (s 133)?
- Can the agency account for its use and communication of lawfully accessed information?

Records checks in the following areas:

- Spot-check only: Whether the use, communication or recording of lawfully accessed information can be accounted for in accordance with ss 139 to 142A
- Whether accessed stored communications were destroyed in accordance with s 150

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

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

Process checks:

- Does the agency have effective procedures in place for applying for and giving preservation notices?

Records checks in the following areas:

- Whether the agency was authorised to give the preservation notice (s 107J(1) or s 107N(1))
- Whether the preservation notice only requested preservation for a permitted period (s 107H(1) or s 107N(1))
- Whether the preservation notice only related to one person and / or one or more services (s 107H(3) or s 107N(2))
- Whether the preservation notice was only issued after the relevant conditions had been met (s 107J(1))
- Whether the preservation notice was given by an authorised officer (s 107M or s 107S)

3.2 Did the agency revoke preservation notices when required?

Process checks:

- Does the agency have effective procedures in place for revoking preservation notices?

Records checks in the following areas:

- Whether the preservation notice was revoked in the relevant circumstances (s 107L or s 107R)
- Whether the preservation notice was revoked by an authorised officer (s 107M or s 107S)

4. Has the agency satisfied certain record keeping obligations?

Process checks:

- Does the agency have processes in place which enable it to accurately report to the Minister on the number of preservations notices given and warrants issued (s 159)?
- Does 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

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 – Telecommunications data inspection criteria 2019-20

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

Specific to prospective authorisations

- 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 s 186A(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)

4. Has the agency satisfied certain record keeping obligations?

Process checks:

- Does the agency have processes in place which enable it to accurately report to the Minister on the number of authorisations made and journalist information warrants issued (s 186)?
- Does the agency have effective record-keeping practices in place?

Records checks in the following areas:

- Whether the agency sent an annual report to the Minister on time in accordance with s 186
- Whether the agency has kept records in accordance with s 186A

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 C – Glossary

Term (and section of the Act)	Description
AAT	Administrative Appeals Tribunal.
Accessing 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*	Under the *Administrative Arrangements Order* the Minister for Home Affairs is responsible for the administration of 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.
Agencies we oversee	• 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 (NSW PF) • Northern Territory Police (NT Police) • Queensland Police Service (QPS) • Independent Commissioner Against Corruption (South Australia) (ICAC SA) • South Australia Police (SA Police) • Tasmania Police (Tas Police) • Victoria Police (VIC Police) • Western Australia Police (WA Police)
Officers approved to exercise the authority of stored	Under s 127(1) of the Act the authority conferred by a stored communications warrant may only be exercised by a person in

Term (and section of the Act)	Description
communications warrants s 127	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.
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 a carrier receives notification of an 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 when an authorisation is in force, if satisfied that the disclosure is reasonably necessary for investigating a serious offence (as defined in s 5D of the Act) or an Australian offence that is punishable by imprisonment for at least 3 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 when an authorisation is in force. Matters about which the AFP must be satisfied in making the authorisation are set out in s 180B(3) of the Act.

Term (and section of the Act)	Description
	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 CAC 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 an 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)). Authorised officers are a critical control for ensuring telecommunication data powers are used appropriately.
Better practice suggestion	When referred to within 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 an agency's part.
Carrier stored communications warrant response coversheet	When providing stored communications to an agency the carrier will typically complete an "*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 stored communications on its systems.
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 an 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.

Term (and section of the Act)	Description
CAC 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 IBAC • 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.
Data vetting	Where an agency screens stored communications or telecommunications data received from a carrier to confirm whether the information was provided within the parameters of a valid stored communications warrant or telecommunications data authorisation.
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'. While the Act does not define 'forthwith' an agency may hold itself to a particular timeframe which will guide our assessments. However, we will also consider whether this timeframe is reasonable in the circumstances noting the ordinary definition of 'forthwith' as immediate and without delay. 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

Term (and section of the Act)	Description
	procedures and what we consider to be reasonable in the circumstances.
Disclosure by agencies to the Office	Prior to or during 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 an agency and inspection officers from the Commonwealth Ombudsman. 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 an agency that are relevant to the inspection.
Historic authorisation ss 178, 178A, 179	A historic authorisation enables access to information or documents that came into existence before a carrier receives notification of an authorisation. An authorised officer must not make an 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 inspections report may be formal or streamlined. We prepare formal reports where our inspection identified 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 an 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. 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

Term (and section of the Act)	Description
	straightforward and non-contentious. A streamlined report may make suggestions and better practice suggestions to an agency to assist it in achieving compliance with the legislation. We provide these reports directly to the relevant business area of an agency.
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) where a purpose of accessing the information is 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 an inspection, distinct from disclosed issues, 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 role 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 the 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

Term (and section of the Act)	Description
Pre-inspection data	Data provided by agencies to the Commonwealth Ombudsman prior to an inspection regarding their use of the powers under Chapter 3 or Chapter 4 of the Act in the relevant period.
Prescribed form s 118(1)(a)	A stored communications warrant must be in the prescribed form. The prescribed form of a domestic 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 given by an agency which requires a carrier to preserve stored communications that relate 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 2 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 at any time on or before the day the carrier receives the notice. • Ongoing domestic preservation notice – may only be given by a criminal law enforcement agency that is also an interception agency. These notices require carriers to preserve stored communications it holds at any time from when the carrier receives the notice to end of 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 it holds at any time on or before the day the carrier receives the notice. • Foreign entities who may make a request to the Australian Federal Police to preserve stored communications are a foreign country, the International Criminal Court or a War Crimes Tribunal (s 107P(1) of the Act).
Privacy considerations s 180F	Section 180F of the Act outlines the privacy considerations that must be made by an authorised officer before making a telecommunications data authorisation. The authorised officer considering making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use 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

Term (and section of the Act)	Description
	• the seriousness of any pecuniary penalty in relation to which the authorisation is sought • the seriousness of any protection of the public revenue in relation to which the authorisation is sought • whether the authorisation is sought for the purposes of finding a missing person • the likely relevance and usefulness of the information or documents • the reason why the disclosure or use concerned is proposed to be authorised.
Prospective authorisation s 180	A prospective authorisation enables access to information or documents that come into existence when an 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 when a person (usually a carrier) receives notification of the authorisation. 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 longer 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 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. The purpose of quarantining information is to prevent any use, communication or disclosure of that information. 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.

Term (and section of the Act)	Description
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 of 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 compliance issue or finding that our Office has made from 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 an 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 review the previous financial year's records during an inspection. During our inspections conducted in the 2019–20 financial year we primarily reviewed records for the 2018–19 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(1)(b) or (c) of the Act are no longer satisfied or if the agency decides not to apply for a warrant to access the preserved stored communications. A domestic preservation notice is revoked by the issuing agency giving the carrier to whom it 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 (s 107L(1) of the Act). <u>Stored communications warrants</u>

Term (and section of the Act)	Description
	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. 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 an authorisation if they are satisfied that the disclosure is no longer required or if the authorisation is made under a JIW, the warrant is revoked.
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 and insider trading.
Standard Operating Procedures (SOPs)	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

Term (and section of the Act)	Description
	(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 authorises approved persons to access 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 relation to a victim of a serious contravention s 116(1)(da)	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 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 its compliance with the Act. Suggestions may include but are not limited to: • updating standard operating policies and procedures • seeking legal advice • training 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 an 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

Term (and section of the Act)	Description
	• the amount of data up / downloaded • the location of a mobile device from which a communication was made.
Telecommunication service carriers	Carriers and carriage service providers who supply 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.
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)	Agencies must keep documents or other materials that indicate whether communicating, using or recording lawfully accessed information under Chapter 3 of the Act 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 **not** 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.