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 inspections conducted in the period 1 July 2021 to 30 June 2022
covering records from 1 July 2020 to 30 June 2021

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 inspections conducted in the period 1 July 2021 to 30 June 2022
covering records from 1 July 2020 to 30 June 2021

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

COMMONWEALTH
OMBUDSMAN

WHAT ARE STORED COMMUNICATIONS?

Communications that already exist and are stored on a carrier's systems. They contain the content of the communication and include items like emails and text messages.

WHAT IS TELECOMMUNICATIONS DATA?

Information about a communication, commonly referred to as 'metadata'. It does not include the content of the communication and includes subscriber information, or the date, time and duration of a communication.

KEY ISSUES

Telecommunication Data

- accessing data where the offence thresholds were not met
- insufficient authorised officer considerations
- inadequate data vetting
- insufficient controls to ensure officers consider whether a Journalist Information Warrant (JIW) may need to be sought
- use and disclosure of telecommunications data not being adequately recorded
- gaps in training and guidance material
- accessing telecommunications data for purposes not provided for in the legislation
- discrepancies in agencies' reporting on the use of telecommunications data powers

Stored communications

- not destroying information received under a stored communications warrant
- warrants relating to a victim needing to demonstrate it was not possible or impracticable to seek the victim's consent
- insufficient record-keeping for use of stored communications

KEY MESSAGES

- We have seen less need to make recommendations, suggestions and better practice suggestions about access to stored communications and telecommunications data in the 2021-22 inspection period compared with the 2020-21 inspection period.
- All agencies were maturing their compliance culture and self-initiating good practices to identify and remedy compliance risks. Many agencies are proactively disclosing and promptly addressing compliance issues.
- Instances continue to be identified where remedial action to previous compliance findings was insufficent.

Executive Summary

This report presents the results of inspections conducted by the Office of the Commonwealth Ombudsman (our Office) under s 186B of the *Telecommunications (Interception and Access) Act 1979* (the Act) from 1 July 2021 to 30 June 2022. These inspections examined agencies' records relating to stored communications and telecommunications data for the period 1 July 2020 to 30 June 2021.

Our Office provides independent oversight of agencies' use of these covert and intrusive powers by inspecting 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 Attorney-General (as the relevant Minister) is required to table in Parliament.

In 2021–22, we inspected 16[1] of the 20 agencies able to exercise stored communications powers under Chapter 3 of the Act. We inspected all 21 agencies able to exercise telecommunications data powers under Chapter 4 of the Act.

During our 2021–22 inspections, we were encouraged that many of the agencies proactively identified and disclosed compliance issues and, where we identified issues during the inspection, sought to address these issues promptly. We found agencies were receptive to our findings, expressing a commitment to strengthening their culture of compliance.

In the reporting period we observed agencies' improved policies, procedures, and controls to mitigate risks of non-compliance based on findings from our previous inspections. The reduction can also be attributed to all agencies maturing their compliance culture and self-initiating good practices to proactively identify and remedy compliance risks. This included, but was not limited to, disclosing instances of non-compliance to our Office, strong procedures supporting the use of stored communications powers, continual improvement of compliance practices and appropriate and timely remedial action taken to previous findings.

There was a decrease in the number of compliance-related findings we made in 2021-22 compared to the 2020-21 inspection period:

[1] We did not inspect the following agencies under Chapter 3 of the Act as these agencies did not exercise these powers during the record period of 1 July 2020 to 30 June 2021: Australian Securities and Investments Commission (ASIC), Independent Broad-based Anti-Corruption Commission (IBAC) and Corruption and Crime Commission (Western Australia) (CCC WA). We also did not inspect South Australia Police (SA Police) in 2021-22 due to COVID-19 travel and border restrictions.

Year	Recommendations	Suggestions	Better Practice Suggestions
2021-22	13 (4 agencies)	145	97
2020-21	29 (6 agencies)	397	116

However, we continued to identify instances at some agencies where we were not satisfied with the remedial action an agency took in response to previous compliance findings, including only partially implementing our previous recommendations and suggestions. Where we were not satisfied with an agency's progress, we re-iterated or made further recommendations or suggestions aimed at improving processes to prevent recurrence of previously identified issues.

Key Inspection Issues	
Stored Communications	**Telecommunication Data**
• agencies not destroying records of information received under a stored communications warrant in line with the Act • the need for agencies applying for warrants relating to a victim of a serious contravention to demonstrate it was not possible or it was impracticable to seek the victim's consent • agencies not keeping sufficient records of their use of stored communications powers as required by the Act	• access to data where the relevant offence thresholds were not met • insufficient information to demonstrate authorised officer considerations • inconsistent or inadequate vetting and quality assurance processes to check data received from telecommunications providers • inconsistent or inadequate agency controls and procedures to ensure officers consider whether a Journalist Information Warrant (JIW) may need to be sought • inconsistent or inadequate record-keeping about use and disclosure of data received under a telecommunications data authorisation • gaps in agency training and guidance material • authorisations for access to telecommunications data being made for purposes not provided for in the Act • discrepancies in agencies' annual reporting on the use of telecommunications data powers to the responsible Minister.

Part A – Introduction

The Commonwealth Ombudsman is responsible for assessing agencies' compliance with Chapter 3 (preserving and accessing stored communications) and Chapter 4 (access to telecommunications data) of the Act.

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

An agency must apply to an external issuing authority (such as a judge or eligible member of the Administrative Appeals Tribunal, or AAT) 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 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. Telecommunications data includes, but is not limited to:

- subscriber information (for example, the name, date of birth and address of the person to whom a service is subscribed)
- date, time, and duration of a communication
- phone number or email address of the sender and recipient of a communication
- Internet Protocol (IP) address used for a session
- start and finish time of each IP session
- amount of data uploaded/downloaded
- location of a device from which a communication was made (this may be at a single point in time, or at regular intervals over a period).

Agencies may internally authorise access to telecommunications data without applying to an external issuing authority, subject to several conditions and requirements. However, if an agency wishes to access the telecommunications data of a person working as a journalist or their employer, and a purpose of the agency is to identify a source, the agency must apply to an external issuing authority and be issued a Journalist Information Warrant (JIW) before it can make such an authorisation[2].

[2] The external issuing authority for a JIW must be a Part 4-1 issuing authority, as specified in s 6DC of the Act. This may include a judge, magistrate, AAT member, legal practitioner of the Federal or Supreme court, who has been enrolled for at least 5 years and appointed in writing by the Attorney General.

Access to stored communications and telecommunications data intrudes on an individual's right to privacy and occurs covertly. The individual generally does not know the agency has accessed their communications or data. This means the individual cannot access complaint or other review mechanisms that would ordinarily be available where they consider an agency has acted unreasonably. Our Office's independent oversight provides assurance to the Parliament and the public about agencies' use of these powers.

Our Office inspects agencies' records and engages with agency staff to assess the extent of compliance with the Act when agencies use these powers. The Act imposes requirements that agencies must satisfy, such as the requirement to weigh the potential value of the information to be obtained against the reasonableness and proportionality of the intrusion on a person's privacy. If agencies cannot demonstrate they are acting consistently with their legislative obligations – including through the records agencies have kept of their use of powers and how they have managed and used the information received – we cannot assure the Parliament and the public that these agencies are using intrusive and covert powers appropriately.

Our inspections 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 was previously identified and not resolved, the Ombudsman may make formal recommendations for remedial action. When an issue of strict non-compliance is less serious or was not identified before, in the first instance we generally 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 risk of non-compliance in the future.

We provide agencies with our preliminary inspection findings verbally at an exit interview and invite agency staff to provide initial comments. We then provide the agency with a written report containing the results of our inspection and our assessment of its legislative compliance. Consistent with procedural fairness principles, the agency has an opportunity to respond to that report and provide comment.

Each year, the Ombudsman is required to report the results of our inspections to the responsible Minister (currently the Attorney-General), who must table the report in the Parliament. We use our individual inspection reports to agencies as the basis to prepare the Ombudsman's consolidated report to the Attorney-General.

As is the case in every reporting period, we made findings in relation to most agencies whose records we inspected during 2021–22. Our findings related not only to issues with agencies' compliance with legislative requirements, but also

areas where agencies can take action to manage risks and continuously improve. In Parts B, C and D, we include specific examples drawn from our inspections of agencies. We emphasise that these examples are illustrative of findings or risks that can be relevant to several agencies that exercised powers under Chapters 3 and 4 of the Act, not just the agency about which the examples are written.

Agencies we oversee

During the 2021–22 record period, 20 agencies could seek access to stored communications and 21 agencies could seek access to telecommunications data under the Act (see table in **Appendix B**). The responsible Minister may declare additional agencies in prescribed circumstances. On 9 February 2022, the then Minister for Home Affairs (who was, at that time, the Minister responsible for the Act) declared Corrective Services NSW (CSNSW) to be an enforcement agency, subject to conditions. This declaration empowered CSNSW to access 'historic' telecommunications data under Chapter 4 of the Act, except in any circumstance where a JIW would be required.

We do not have jurisdiction to oversee the activities of telecommunication service carriers, which hold the telecommunications data that agencies seek access to (for example, Telstra and Optus). Pursuant to s 309 of the *Telecommunications Act 1997* (Cth), the Information Commissioner has the power to monitor compliance with Part 13, Division 5 of the that Act, which requires carriers and carriage service providers to record certain disclosures of personal information, including disclosures of telecommunications data collected and retained under the data retention scheme, to law enforcement agencies. The Information Commissioner also has the power to monitor these entities' compliance with their obligations under the *Privacy Act 1988* (Cth).

Inspections conducted in 2021-22

In 2021–22, our Office conducted inspections of 16 agencies' use of stored communications powers under Chapter 3 of the Act, and inspections of 21 agencies empowered to use telecommunications data powers under Chapter 4 of the Act.

The Act does not specify the frequency of inspections under Chapter 3 or 4. Our Office scheduled inspections for all agencies which used the stored communications and telecommunications data powers during the record period 1 July 2020 to 30 June 2021. In addition to the pre-scheduled inspections, we also conducted a 'health check' inspection of CSNSW, which had not used the powers during the record period.

Due to COVID-19 restrictions, we conducted some inspections remotely. We acknowledge and appreciate the assistance those agencies provided in preparing for and working with our office during remote inspections.

Own motion investigation
During our scheduled inspection of the use of telecommunications data powers by the Australian Federal Police (AFP), our Office also took the opportunity to review the AFP's progress in addressing the recommendations made in our April 2021 report on the AFP's use and administration of telecommunications data powers 2010 to 2020.

We noted the significant reform work undertaken and were satisfied the AFP had addressed 4 of the 8 recommendations, with the remaining items well progressed. We found further action was required to fully address the remaining recommendations, including demonstration of a more integrated and consistent approach to managing telecommunications data access processes across the AFP. We will assess further progress made at our 2022-23 inspection.

How we oversee agencies
We apply a set of inspection methodologies consistently across agencies. These methodologies are based on the legislative requirements of the Act and better practice standards. We update our methodologies in response to legislative amendments and changes to agency processes.

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

We provide our inspection criteria to agencies before each inspection. This helps agency staff identify the most accurate sources of information to assist our inspection. We encourage agencies to proactively disclose any non-compliance, including remedial action they have already taken.

Our Office also seeks to support compliance by assessing agencies' policies, procedures and training, communicating better practices, and facilitating communication across agencies that use the same powers.

For agencies granted new access to powers, we conduct a 'health check' inspection aimed at assessing the readiness or 'health' of an agency's compliance framework. We focus on determining whether the frameworks, policies and procedures an agency has developed, or are in the process of developing, are suitable for supporting compliance with the Act.

Risk Based Oversight
During the 2021-2022 inspection period, our Office commenced work on developing a risk based approach to compliance inspection under the Act. This approach allows our Office to better target practices, processes and records which

present the highest risk of non-compliance and to provide more meaningful assurance to Parliament and the public on agencies use of covert, coercive and intrusive powers.

Our office has commenced a trial of this risk based approach with our 2022-2023 inspections of agencies use of powers under Chapter 4 of the Act. While we continue to inspect all agencies during this current inspection period, the trial will explore the extent to which a number of key risk activities occur both within and across inspected agencies. The outcomes from this trial will be reported in next year's annual report.

Stakeholder engagement

During 2021–22, we provided information and compliance feedback to agencies about emerging compliance risks and better practice in exercising the powers under Chapters 3 and 4 of the Act. This included presentations at agency training, providing compliance feedback on changes to agency templates, guidance or procedures, and other compliance advice to support agencies. This engagement outside of inspections helps our Office obtain a greater understanding of the issues faced by agencies when using the powers. It also enables our Office to notify agencies of emerging risks to non-compliance identified through our oversight.

Part B – Culture of compliance

During our inspections of an agency's use of powers under Chapters 3 and 4 of the Act, we assess compliance with the Act against our inspection criteria. The number of findings identified during an inspection is not a precise indicator of the strength of a compliance culture, noting that the degree and significance of non-compliance varies depending on the nature of the finding, the frequency with which an agency uses the powers, an agency's practices, processes and training, and agency's management of compliance with the Act.

When assessing whether an agency has a strong compliance culture, we consider whether it:

- undertakes regular training for officers involved in exercising powers
- provides support and appropriate guidance material for officers involved in exercising powers
- proactively identifies and takes action to resolve compliance issues
- discloses issues to our Office
- addressed issues identified at previous inspections, and
- engages in a frank and responsive manner during our inspections.

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

In 2021–22, we were pleased to observe several good practices among agencies, notably the establishment or continuation of centralised compliance functions. We were also pleased to observe several practices indicating a maturing compliance culture. Such practices included, but were not limited to, disclosing instances of non-compliance to our Office, strong procedures supporting the use of stored communications powers, continual improvement to compliance practices and appropriate and timely remedial action taken to previous findings.

Improving compliance culture – Tasmania Police

Prior to our 2021-22 inspection period, Tasmania Police received 3 formal reports from our Office regarding serious or repeat issues of non-compliance in the use of powers under Chapter 3 and Chapter 4 of the Act. Following our 2020-21 report, Tasmania Police dedicated effort to improve stored communications and telecommunication data governance and address the previous recommendations, suggestions and better practice suggestions.

On our 2021-22 inspection, we found Tasmania Police had undertaken significant work to improve policies and guidance relating to stored

communications and telecommunication data, developed training that covered Chapter 3 and 4 of the Act and updated templates for applications and warrants for stored communications. Following the inspection, Tasmania Police sought advice from our Office on proposed changes to their systems used to request, authorise, record and manage access to telecommunication data. This included improving the Tasmania Police's recording of authorising officer consideration of privacy, relevance and any requirement for a JIW under Chapter 4 of the Act.

As a result, we made only one finding on this inspection relating to Tasmania Police's access to stored communications, stemming from a self-disclosure by the agency, which we believed the remedial action already undertaken would address the issue for future inspections. We made 5 suggestions in relation to accessing telecommunication data, 3 of which recognised and supported Tasmania Police continuing their work to improve their compliance frameworks, governance and training.

The significant reduction in inspection findings in 2021-22 reflects the work of Tasmania Police in improving its stored communications and telecommunication data regimes.

Part C – Stored communications

Stored communications and the Commonwealth Ombudsman's oversight function

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

To access stored communications, an agency must apply to an external issuing authority (such as a Judge or eligible 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 specified on the warrant.

Before a warrant is issued, an agency may authorise the preservation of a stored communication. This ensures the relevant 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, and
- foreign preservation notices (only available to the AFP).

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 agencies' applications for stored communications warrants and accompanying affidavits to assess whether agency processes comply with the requirements of Chapter 3 of the Act. This includes whether the agency provided the issuing authority with sufficient and accurate information to make the required considerations when deciding whether to issue a stored communications warrant.

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

Other matters our Office assesses include, but are not limited to, how agencies manage access to stored communications, and agencies' compliance with record-keeping and reporting obligations. Our inspections criteria for stored communications inspections conducted in 2021–22 is set out at **Appendix C**.

Summary of stored communications findings

During 2021–22, our Office inspected 16 agencies' access to stored communications under Chapter 3 of the Act. For all agencies our inspections covered records for the period 1 July 2020 to 30 June 2021. For our stored communications inspections conducted during 2021–22 we made:

- 2 recommendations to one agency
- 21 suggestions, and
- 19 better practice suggestions.

This reflects a significant decrease compared to our inspections in 2020–21, where we made 6 recommendations to 3 agencies, 124 suggestions and 49 better practice suggestions.

All agencies were receptive to our findings and, in some instances, the agency immediately took remedial actions during our inspection to address identified issues. Several of our findings related to issues proactively identified and disclosed by agencies, ranging from minor administration errors to more significant compliance matters.

Although we were satisfied with the remedial action taken by many agencies in response to our previous inspection findings, there were several agencies where issues re-occurred. While some of these re-occurring issues arose due to the retrospective nature of our inspections, there were a small number of instances where we were not satisfied with the remedial action taken by agencies[3]. In such instances, we made further suggestions or recommendations including improving processes to prevent reoccurrence of the issue.

To prevent repeated findings over sequential inspections, our Office encourages agencies to consider feedback we provide and to implement measures to address identified issues in a timely manner. It is also open to agencies to seek early views and compliance feedback from our Office outside our standard inspection schedule as they implement mechanisms to improve compliance.

Recommendations and suggestions made during 2021–22

The table below sets out the number of recommendations, suggestions and better practice suggestions made by our Office to each agency during this period. For most agencies, we saw a decrease in the number of recommendations, suggestions and better practice suggestions made. It is important to note that, where we saw an increase, this does not necessarily translate to poorer compliance on behalf of an agency, as findings vary in their impact and level of

[3] AFP and NSWCC

risk. For example, an agency may have a higher number of minor impact or low risk findings, but less findings on issues with significant impact or higher risk.

Table 1 – Number of recommendations, suggestions, and better practice suggestions made per agency during the 2021–22 inspection period (figures from the 2020–21 inspection period are included in brackets)

Agency	Recommendations	Suggestions	Better Practice Suggestions	Total
Australian Competition and Consumer Commission	0 (0)	1 (8)	1 (3)	2 (11)
Australian Criminal Intelligence Commission	0 (0)	1 (4)	1 (2)	2 (6)
Australian Commission for Law Enforcement Integrity	0 (0)	1 (6)	0 (1)	1 (7)
Australian Federal Police	2 (2)	4 (22)	3 (6)	9 (30)
Crime and Corruption Commission (Queensland)	0 (0)	1 (1)	0 (2)	1 (3)
Corruption and Crime Commission Western Australia[4]	0 (0)	0 (0)	0 (0)	0 (0)
Department of Home Affairs	0 (0)	4 (4)	4 (5)	8 (9)
Independent Broad-base Anti-corruption Commission[5]	0 (0)	0 (4)	0 (2)	0 (6)

[4] There were no findings for our inspection conducted in 2020-21 and no inspection in 2021–22 as the agency did not use the powers under Chapter 3 of the Act during the relevant records period.

[5] No inspection conducted in 2021–22 as the agency did not use the powers under Chapter 3 of the Act during the relevant records period.

Agency	Recommendations	Suggestions	Better Practice Suggestions	Total
Independent Commission Against Corruption New South Wales	0 (0)	0 (10)	2 (2)	2 (12)
Independent Commissioner Against Corruption (South Australia)	0 (0)	0 (0)	1 (0)	1 (0)
Law Enforcement Conduct Commission	0 (0)	1 (12)	0 (4)	1 (16)
New South Wales Crime Commission	0 (0)	2 (1)	2 (2)	4 (3)
New South Wales Police Force	0 (0)	0 (4)	0 (2)	0 (6)
Northern Territory Police	0 (0)	4 (5)	0 (2)	4 (7)
Queensland Police Service	0 (0)	1 (2)	1 (1)	2 (3)
South Australia Police	0 (0)	0 (10)	0 (1)	0 (11)
Tasmania Police	0 (1)	0 (12)	0 (8)	0 (21)
Victoria Police	0 (3)	1 (10)	1 (4)	2 (17)
Western Australia Police	0 (0)	0 (9)	3 (2)	3 (11)
TOTAL:	**2 (6)**	**21 (124)**	**19 (49)**	**42 (179)**

We did not inspect SA Police in 2021–22 due to COVID-19 risk considerations at the time the inspection was scheduled. Instead, we conducted a telephone consultation with key staff at SA Police to discuss progress made on findings from

the previous inspection. We inspected SA Police's use of stored communication powers early in 2022–23, the results of which will be reflected in our 2022–23 annual report.

Table 2 – Use of stored communications powers and records inspected in the 2021–22 period

Agency	Records period inspected	Total Historic PN[6]	Historic PN Inspected	Total Ongoing PN	Ongoing PN inspected	Stored Comms Warrants[7]	Warrants inspected	Destructions	Destructions inspected
ACCC	20-21	8	**8**	-	**-**	-	**-**	-	**-**
ACIC	20-21	-	**-**	5	**5**	1	**1**	-	**-**
ACLEI	20-21	-	**-**	1	**1**	-	**-**	-	**-**
AFP	20-21	69	**8**	100	**34**	88	**24**	67	**11**
CCC QLD	20-21			62	**45**	1	**1**	14	**14**
Department of Home Affairs	20-21	2	**2**	-	**-**	1	**4**	-	**-**
ICAC NSW	20-21	-	**-**	1	**1**	-	**-**	-	**-**
ICAC SA	20-21	1	**1**	13	**13**	2	**2**	-	**-**
LECC	20-21	1	**1**	16	**16**	9	**9**	-	**-**
NSW CC	20-21	1	**1**	3	**3**	1	**1**	-	**-**
NSW PF	20-21	436	**39**	162	**7**	489	**42**	-	**-**
NT Police	20-21	42	**42**	9	**9**	1	**1**	-	**-**
QPS	20-21	73	**13**	168	**34**	129	**42**	141	**43**
Tasmania Police	20-21	31	**2**	54	**14**	43	**21**	45	**17**
Victoria Police	20-21	91	**20**	69	**19**	102	**37**	59	**36**
WA Police	20-21	125	**12**	109	**8**	87	**16**	16	**8**
Total		**880**	**149**	**772**	**209**	**954**	**201**	**342**	**129**

[6] This is the total of Preservation Notices (PN) reported to our Office. In some instances, this did not reflect the actual number of preservation notices given by the agency during the financial year 2020–21. This is because a preservation notice may still be in force during our inspection and will be subject to compliance assessment on expiration in our next records period, or because an agency has incorrectly reported on the number of preservation notices to our Office.

[7] This is the total of warrants reported to our Office. In some instances, this did not reflect the actual number of warrants issued to the agency during the financial year 2020–21. This occurs where a warrant may still be in force during our inspection and will be subject to a compliance assessment on expiration in our next records period, or because an agency has incorrectly reported on the number of warrants to our Office.

Compliance issues and risks to compliance

This section outlines instances of non-compliance identified across multiple agencies during the 2021–22 stored communications inspections, and issues that may pose a risk to compliance. We will review agencies' actions in response to these issues and all other findings from the 2021–22 reports at future inspections.

Our inspections revealed several key areas that we consider pose the greatest risk to an agency's compliance with the Act. These included findings regarding:

- destruction of stored communications
- special considerations when applying for a stored communications warrant for a victim of a serious contravention, and
- record keeping requirements regarding the use of stored communications powers.

Systemic issues regarding the handling of foreign preservation notices and warrants

Section 107P of the Act enables specified international entities to request the preservation of stored communications held by Australian carriers that relate to a specified person in connection with a serious contravention of foreign laws. Only the AFP may give foreign preservation notices.

In our 2020–21 report, we recommended the AFP implement a centralised and specialised quality assurance process with respect to issuing foreign stored communications warrants and foreign preservation notices and the subsequent management and use of stored communications received under a warrant. This recommendation was made in response to significant shortcomings identified in relation to the AFP's management of foreign preservation notices and foreign stored communications warrants across several inspection periods dating back to 2018-19.

The AFP has since amended its practices, so a centralised area now manages quality assurance for all foreign preservation notices and warrants. However, during our 2021–22 inspection, we still observed a lack of guidance on how to conduct quality assurance, particularly in relation to foreign preservation notices and foreign stored communications warrants. We could only identify one document used in the AFP's National Special Projects Registrar (SPR) quality assurance process which was inconsistent with the AFP's policies or procedures.

While the AFP had taken some action in response to our previous recommendation, we were not yet satisfied that sufficient action has been taken. We reiterated our previous recommendation that the AFP implement a centralised and specialised quality assurance process with respect to issuing foreign stored communications warrants and foreign preservation notices, and the subsequent management and use of stored communications received.

In response, the AFP advised that training has been delivered on quality assurance requirements and to ensure staff are aware of the amended practices centralising this process. The AFP has also introduced a quality assurance checklist for warrant affidavits and will create a quality assurance checklist for foreign preservation notices. The AFP also advised it will review and update all governance documentation to ensure it consistently reflects the new centralised quality assurance process.

Destructions 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 likely to be 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. This includes that no stored communications should be destroyed without appropriate written approval from the chief officer.

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

The Act does not require periodic reviews of stored communications information or records to consider if any information or records should be destroyed under s 150(1) of the Act. However, for best practice it is our position that agencies should periodically consider and review whether such information or records are still likely to be required for a permitted purpose. This is due to the privacy intrusion associated with continued retention of stored communications information.

We consider a destruction to be complete when all steps in a destruction process are finalised. This includes confirmation of destruction by the agency of all information or records that were obtained by accessing stored communications (including any copies and computer records as per the definition of a record in s 5(1) of the Act).

Achieving compliance with destruction requirements requires agencies to:

1. have a strong framework in place to track all relevant stored communications

2. seek appropriate approval for destruction from the chief officer or their delegate
3. ensure destruction of relevant records and information (including copies) forthwith.

Where an agency has a process of identifying and locating relevant information and records prior to seeking chief officer approval, the agency is well placed to meet the forthwith requirement. Robust record-keeping and document tracking processes reduce delays in accounting for records after the chief officer certifies 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.

During our 2021–22 inspections we made 4 suggestions and 3 better practice suggestions across 5 agencies[8] regarding destruction of stored communications. Our suggestions and better practice suggestions included:

- ensuring destruction reports are provided to the Minister in accordance with the requirements under s 150(2) of the Act
- ensuring sufficient records are kept demonstrating whether stored communications were destroyed in accordance with s 150 of the Act
- finalising and updating destruction policies and procedures to ensure the agency can comply with legislative requirements
- the interaction between positive requirements to destroy stored communications if not likely to be required for a purpose referred to in s 150 of the Act and obligations to keep records of investigations to comply with State record-keeping legislation.

There has been a sizeable decrease in the number of destruction related findings in 2021–22, as a result of improvements generally among agencies who have actioned our previous findings. In our 2020–21 annual report we reported on 20 suggestions and 14 better practice suggestions regarding destruction of stored communications across 14 agencies.

Need for established destruction policies and procedures to support compliance

During our 2020–21 inspection, we found the Department of Home Affairs (Home Affairs) had not finalised its destructions policy and no destructions of stored communications had been undertaken. We suggested it finalise its destructions policy and draft standard operating procedures.

[8] AFP Home Affairs, ICAC NSW, NSW CC, WA Police.

At the time of our 2021–22 inspection, Home Affairs had not yet finalised its destruction policy and had not conducted any destructions of stored communications.

While the Act does not require periodic reviews of stored communications to consider if any information or records should be destroyed under s 150(1) of the Act, it is our position that an agency's practices should include periodic consideration and review of whether such information or records are still likely to be required for a permitted purpose. This is particularly important given the high level of privacy intrusion associated with stored communications information. We reiterated our previous suggestion that the department finalise its destructions policy and standard operating procedure as a priority.

Home Affairs accepted this suggestion advising that it has settled its policy position and is in the process of developing/amending procedural documents.

Ensuring policy and procedures accurately reflect destruction requirements

During our inspection of the NSW CC, we reviewed its destruction procedures. The procedures advised that no stored communications product can be destroyed until inspected by the Ombudsman and directed to be disposed by the Ombudsman.

We advised the NSW CC that there is no legislative requirement to retain stored communications product until it is inspected by our Office. Authorisations for destruction should be sought as soon as possible once it is identified that stored communications or records are no longer required for a purpose specified in s 150(1) of the Act.

We suggested that the NSW CC update its policy and procedures to accurately reflect the requirements for destroying all stored communications records forthwith in accordance withs 150(1) of the Act.

In response, the NSW CC advised that it has actioned this suggestion.

When a stored communications warrant can be applied for in relation to a victim of a serious contravention

Section 116(1) of the Act lists the matters of which an issuing authority, based on the information given to them with the application, must be satisfied in issuing a stored communications warrant. Subject to meeting all other requirements, this includes that an issuing authority may issue a stored communications warrant in relation to a victim of a serious contravention if satisfied the person is 'unable' to consent, or it is 'impracticable' for the person to consent to those stored communications being accessed.

It is our view that a person would be deemed 'unable to consent' where, for example, they are missing and cannot be located, or are incapacitated or deceased. Obtaining consent would be deemed 'impracticable' where a person's situation makes contacting them extremely difficult, time-consuming, or disproportionately expensive. If a victim has an opportunity to consent and they do not wish their stored communications to be accessed, then an agency generally should not use s 116 of the Act to access their stored communications. If a victim declines to give their consent, the view of our Office is that their reasons for doing so are immaterial.

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

In instances where there is limited information in the affidavit explaining why the agency determined that it is impracticable to seek consent, or that the victim is unable to consent, we consider the issuing authority may not have been provided with all relevant information to determine whether to issue the warrant in light of s 116(1)(da) of the Act.

We made 5 suggestions and 1 better practice suggestion across 4 agencies[9] during our 2021-22 inspections relating to when a stored communications warrant can be applied for in relation to a victim of a serious contravention.

Our suggestions and better practice suggestion included:

- clearly demonstrating how the thresholds of 'unable' or 'impracticable' have been met when apply for a stored communications warrant in relation to a victim
- enhancing guidance and raising staff awareness on circumstances where the thresholds of a victim being unable to consent, or where it is impractical for the victim to consent, could be met, and
- seeking legal advice on a practice of seeking stored communications warrants where the victim has consented to stored communications being accessed.

[9] The AFP, Home Affairs, QPS, NT Police.

There has been an increase in the number of findings in relation to this topic in 2021–22, and this will continue to remain an area of focus for our office at future inspections.

Seeking stored communications warrants where the victim has consented to stored communications being accessed

During our 2021–22 inspections, we suggested the AFP and NT Police seek legal advice regarding the seeking of stored communications warrants in relation to victims where the victim has consented to stored communications being accessed. The agency should also implement further updates to templates, guidance, and procedural material if the advice is that a stored communications warrant under Chapter 3 of the Act is not required – or cannot be issued –where a victim has consented to the agency accessing their stored communications. We also suggested that both agencies enhance guidance and raise staff awareness of the circumstances where the thresholds of a victim being unable to consent, or where it is impractical for the victim to consent, could be met. The particular instances we identified were:

- One instance where the AFP was issued a stored communications warrant regarding a victim where the affidavit stated the victim provided consent to police to examine and acquire their stored communications. The AFP advised it does not routinely obtain stored communications warrants for victims where they consent to police accessing their data, but the carrier advised the AFP that if a preservation notice is served on them, stored communications will only be available through a stored communications warrant.

- We found that NT Police's template and guidance request officers gain consent from all victims prior to accessing stored communications under s 116 of the Act.

In response to our suggestion, the AFP advised that it had obtained legal advice and updated its template and quality assurance checklists accordingly. The AFP has also undertaken to update its governance documentation to ensure it correctly reflects the requirements of s 116(1)(da) of the Act. NT Police acknowledged our findings and advised it would continue to address the matters raised in our report.

Stored communications warrant obtained

We identified one instance at the QPS where a stored communications warrant was applied for, and granted, in relation to a victim of a serious contravention. The QPS advised that, at the time the preservation notice was given prior to the warrant application, the victim was unable to give consent. However the warrant affidavit

stated that, after the preservation notice had been given, the victim had provided a statement to the QPS.

We advised the QPS that s 116(1)(da) of the Act is applicable to the ability of the victim to give consent at the time the warrant is applied for, and that in our view the application for the warrant did not meet the requirements of the Act. We advised the QPS to quarantine the stored communications and seek legal advice on the management of any use or communication. The QPS advised our Office that the information obtained under the warrant had not been used or communicated.

We suggested that, where a stored communications warrant is being sought in relation to a victim of a serious contravention, the QPS should ensure that affidavits accurately reflect whether consent has been sought. Where consent has not been sought, the QPS should clearly demonstrate how the thresholds of 'unable' or 'impracticable' have been met.

In response, the QPS accepted our suggestion in full and advised it will ensure affidavits adequately address consent if a warrant is sought in relation to a victim of a serious contravention.

Obligation to keep records

Agencies are required under s 151(1) of the Act to keep certain records for the period specified in s 151(3) of the Act. These records include, but not limited to: preservation notices, revocation notices, stored communication warrants, revocation of stored communication warrants, use and communication records, destruction records and reports to the Minister (currently the Attorney-General).

An agency should maintain consistent processes to ensure it meets its obligations under s 151 of the Act to keep records. Record keeping is an important mechanism to ensure there is transparency on the use of these covert and intrusive powers and is necessary to facilitate effective oversight to provide assurance that these powers are being used in accordance with legislation.

During the 2021-22 inspection period, we made 1 suggestion and 4 better practice suggestions across 4 agencies[10] regarding record keeping issues. Our suggestion and better practice suggestions included:

- ensuring agency processes to capture information indicating whether a preservation notice was properly given are consistently followed by staff
- incorporating tools that record use and communication of stored communications into policies, procedures and training to ensure staff awareness of obligations

[10] The ACIC, Home Affairs, Victoria Police, WA Police.

- strengthening guidance to reflect record keeping requirements regarding use and communication fully and accurately, and
- ensuring that records are kept by the agency as required under s 151(1) of the Act, including records indicating whether warrants were properly applied for.

Ensuring processes to consistently capture information to demonstrate preservation notices are properly given are followed

During our inspection of the ACIC, we identified instances where there was insufficient information in the records to demonstrate that a preservation notice was properly given, in particular information demonstrating how the condition under s 107J(1)(c) of the Act to demonstrate reasonable suspicion that stored communications were, or may come into existence during the notice period that might assist in connection with the investigation and, relate to the person or service specified in the notice, was met. We were not satisfied the ACIC was consistently meeting its record-keeping obligations under s 151(1)(a) of the Act.

We previously made this finding to the ACIC in 2020–21, following which the ACIC updated its template forms and included additional guidance to officers. We were satisfied that appropriate completion of the updated form would assist the ACIC in meeting its record keeping obligations.

In 2021–22 we suggested the ACIC ensure its processes (updated in .2020–21) are consistently followed to meet its obligation under s 151(1)(a) of the Act to keep records indicating whether a preservation notice was properly given. This process should capture information relevant to the decision to give a preservation notice and determining whether the conditions for giving a preservation notice are met, as required by s 151(1)(a) of the Act.

In response, ACIC advised it will engage with its staff to address the issue.

Part D – Telecommunications data

Telecommunications data and the Commonwealth Ombudsman's oversight function

Under s 186B(1)(a) of the Act, the Ombudsman must inspect the records of an enforcement agency to determine the extent of compliance with Chapter 4 by the agency and its officers. Under s 186J of the Act, the Ombudsman must report to the Minister on the results of inspections conducted under s 186B after the end of each financial year.

Agencies are empowered to internally authorise access to telecommunications data without applying to a judge or AAT member, subject to several conditions and requirements. To authorise disclosure of telecommunications data, among other considerations, an authorised officer must weigh the likely relevance and usefulness of the disclosed telecommunications data to the investigation against the privacy intrusion it causes.

Under ss 178(2), 178A(2), and 179(2) of the Act, an authorised officer may authorise the disclosure of specified information or documents that came into existence *before* the telecommunications provider receives notification of the authorisation. We refer to this as a 'historic' authorisation. The authorised officer must not make the authorisation unless satisfied the disclosure is reasonably necessary for:

- the enforcement of the criminal law
- finding a person who the agency has been notified is missing
- the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

Similarly, under s 180(2) of the Act, an authorised officer may authorise the disclosure of specified information or documents that come into existence during the period the authorisation is in force. We refer to this as a 'prospective' authorisation. The authorised officer must not make the authorisation unless satisfied the disclosure is reasonably necessary for the investigation of a serious offence or an offence that is punishable by at least 3 years' imprisonment.

Under limited circumstances, access to historical telecommunication data can be provided to foreign law enforcement. Under s 180A of the Act, an authorised officer of the AFP may make an authorisation to access telecommunication data or disclose telecommunication data in possession of the AFP, if it is reasonably necessary for:

- the enforcement of the criminal law of a foreign country
- investigation or prosecution of a crime within the jurisdiction of the International Criminal Court (ICC)
- investigation or prosecution of a War Crimes Tribunal offence.

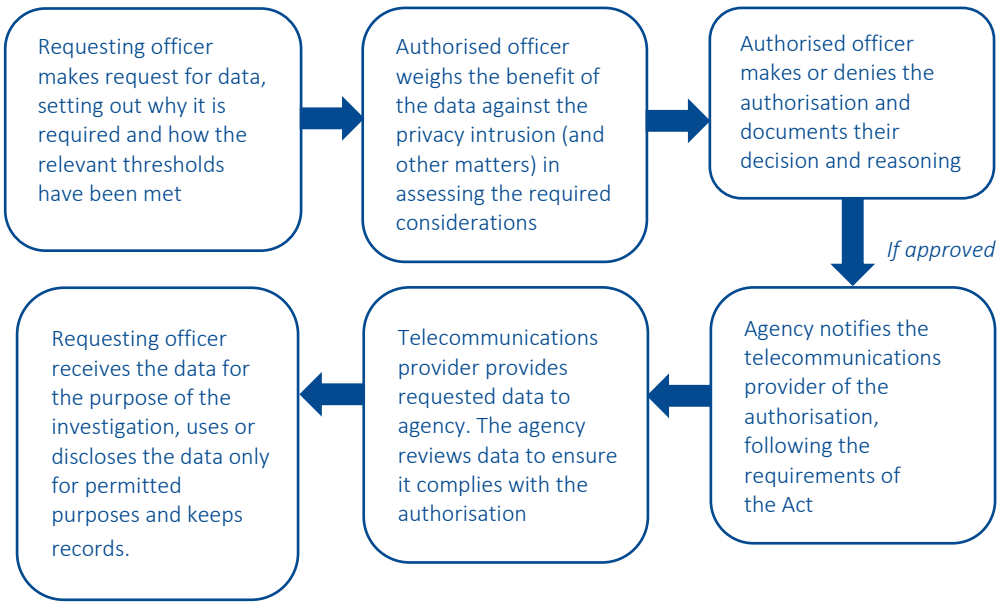
While access to prospective telecommunication data may be authorised under the provisions of s 180B of the Act, the authorisation may only be made if the Attorney-General has authorised the disclosure under the provisions of s 15D of the *Mutual Assistance in Criminal Matters Act 1987* or in the investigation or prosecution of a crime with the jurisdiction of the ICC or a War Crimes Tribunal offence.

Our Office does not review the merits of an authorised officer's decision to authorise disclosures of telecommunications data. We assess whether agencies satisfy the requirements of the Act, which involves assessing there is sufficient information for officers authorising these disclosures to take the required considerations into account.

Only officers authorised by the chief officer of the agency can authorise disclosure of telecommunications data.

If an agency wishes to access the telecommunications data of a person working as a journalist or their employer, and a purpose of the agency is to identify a source, the agency must apply to an external issuing authority and be issued a JIW before it can make such an authorisation.

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 to assess the required considerations under the Act.

We assess the processes agencies have in place to request telecommunications data, make authorisations, notify the carriers, and manage the data once it is received. This includes checking agencies maintain records demonstrating that any disclosure or use of telecommunications data complied with the requirements of the Act.

Summary of telecommunications data findings

During 2021–22, our Office inspected 20 agencies' access to telecommunications data under Chapter 4 of the Act, covering records for the period from 1 July 2020 to 30 June 2021. For our telecommunications data inspections conducted during 2021–22 we made:

- 11 recommendations across 4 agencies
- 124 suggestions, and
- 78 better practice suggestions.

This was a decrease from the 2020–21 inspection period figures of 23 recommendations made across 6 agencies, 273 suggestions and 67 better practice suggestions. We observed efforts made by all agencies to address previous inspection findings, which has reduced the number of findings and repeat issues identified at many agencies in the current period. While this reduction in findings indicates improved compliance by the agencies, we remain concerned about high numbers of suggestions and better practice suggestions demonstrating the need for additional agency improvements.

During 2021–22, we also conducted one health check inspection at Corrective Services NSW (CSNSW), which was newly empowered to access telecommunications data in 2021–22. We reviewed CSNSW's policies, templates and other governance documents, and where relevant, provided compliance feedback to reduce further risks of future non-compliance. Overall, we found that CSNSW's framework for using telecommunications data contained appropriate detail to support use of the powers. However, there were some opportunities for improvement. As a result, we made 11 better practice suggestions to CSNSW to address areas for improvement. CSNSW was responsive to our findings and advised our Office of that actions had been taken to implement the better practice suggestions.

Agencies we inspect are diverse in size and operating environment, which shapes the volume and type of requests made for access to telecommunications data. While all agencies had taken steps to address previous findings, and some demonstrated high levels of compliance with the Act, others had not demonstrated sufficient progress in addressing previous issues identified, resulting in further recommendations and suggestions from our Office.

Agencies where we identified the most non-compliance issues were larger agencies which use telecommunications data powers more frequently and have higher numbers of requesting and authorised officers (commonly geographically dispersed), experiencing regular staff changes. Consequently, officer awareness of the relevant legislative obligations can be harder to maintain, especially where the agency does not provide regular targeted training and comprehensive guidance documentation to support officers to achieve compliance with the Act.

Agencies which experience better compliance had independent quality assurance and data vetting practices to help self-identify and manage compliance issues. These agencies typically established centrally coordinated online request and authorisation systems to improve compliance by streamlining these processes, increasing consistency and improving record-keeping[11].

Recommendations and suggestions made during 2021–22

The table below sets out the number of recommendations, suggestions and better practice suggestions made by our Office to each agency during this period. For most agencies, we saw a decrease in the number of recommendations, suggestions and better practice suggestions made. It is important to note that, where we saw an increase, this does not necessarily translate to poorer compliance on behalf of an agency, as findings vary in their impact and level of risk. For example, an agency may have a higher number of minor impact or low risk findings, but less findings on issues with significant impact or higher risk.

Table 3 – Number of recommendations, suggestions, and better practice suggestions made per agency during the 2021–22 inspection period (figures from the 2020–21 inspection period are included in brackets)

Agency	Recommendations	Suggestions	Better practice suggestions	Total
Australian Competition and Consumer Commission	0 (0)	3 (3)	3 (1)	6 (4)
Australian Criminal Intelligence Commission	0 (0)	6 (8)	11 (4)	17 (12)
Australian Commission for Law Enforcement Integrity	0 (0)	6 (16)	4 (3)	10 (19)
Australian Federal Police	2 (4)	11 (16)	6 (4)	19 (24)
Australian Securities and Investments Commission	0 (0)	0 (10)	0 (7)	0 (17)

[11] Examples of agencies which experience better compliance included ACLEI, ACIC, ACCC, ASIC, IBAC, NSW ICAC, SA ICAC, LECC, NSW CC, QCCC, WACCC, and WA Police

Agency	Recommendations	Suggestions	Better practice suggestions	Total
Crime and Corruption Commission (Queensland)	- (-)	10 (12)	2 (4)	12 (16)
Corruption and Crime Commission (Western Australia)	- (-)	- (5)	3 (1)	3 (6)
Department of Home Affairs	- (-)	6 (12)	9 (7)	15 (19)
Independent Broad-based Anti-corruption Commission	- (-)	5 (30)	- (5)	5 (35)
Independent Commission Against Corruption New South Wales	- (-)	1 (9)	1 (-)	2 (9)
Independent Commissioner Against Corruption (South Australia)	- (-)	7 (7)	4 (1)	11 (8)
Law Enforcement Conduct Commission	- (-)	3 (11)	3 (3)	6 (14)
New South Wales Crime Commission	- (-)	4 (9)	3 (3)	7 (12)
New South Wales Police Force	- (-)	7 (19)	9 (1)	16 (20)
Northern Territory Police	2 (3)	11 (16)	1 (7)	14 (24)
Queensland Police Service	- (2)	4 (11)	2 (-)	6 (13)
South Australia Police	3 (5)	14 (26)	3 (3)	20 (34)

Agency	Recommendations	Suggestions	Better practice suggestions	Total
Tasmania Police	- (6)	5 (14)	- (5)	5 (25)
Victoria Police	4 (3)	7 (22)	5 (4)	16 (29)
Western Australia Police	- (-)	14 (17)	9 (4)	25 (21)
TOTAL:	**11 (23)**	**124 (273)**	**78 (67)**	**215 (363)**

Table 4 – Use of telecommunications data powers and records inspected in the 2021–22 period[12]

Agency	Records period inspected	Total Historic	Historic Inspected	Total Prospective	Prospective inspected
ACCC	20-21	113	**42**	-	**-**
ACIC	20-21	4,060	**23**	1,073	**20**
ACLEI	20-21	184	**13**	40	**11**
AFP	20-21	18,610	**41**	6,838	**22**
ASIC	20-21	622	**41**	124	**33**
CCC QLD	20-21	698	**40**	207	**24**
CCC WA	20-21	191	**26**	87	**16**
Department of Home Affairs	20-21	4,286	**7**	416	**6**
IBAC	20-21	312	**30**	252	**39**
ICAC NSW	20-21	149	**12**	19	**14**
ICAC SA	20-21	175	**16**	52	**13**
LECC	20-21	748	**23**	129	**18**
NSW CC	20-21	3,581	**30**	1,620	**17**
NSW PF	20-21	106,203	**49**	1,479	**19**
NT Police	20-21	2,062	**31**	340	**20**
QPS	20-21	25,909	**8**	4,348	**11**
SA Police	20-21	5,735	**55**	469	**38**
Tasmania Police	20-21	3,982	**25**	114	**40**
Victoria Police	20-21	110,120	**47**	16,671	**35**

[12] The record numbers listed in 'Total Historic' is the number of historic records reported to our Office by the agency pre-inspection, from which we drew our inspection sample. In some inspections, we made findings where the number of historic authorisations reported to our Office did not reflect the actual number of authorisations made by the agency. While the reasons for these differences varied between agencies, we suggested the impacted agency review and appropriately amend their reporting of the number of historic authorisations.

Agency	Records period inspected	Total Historic	Historic Inspected	Total Prospective	Prospective inspected
WA Police	20-21	26,864	**40**	3,951	**26**
Total		**314,607**	**599**	**38,229**	**422**

Journalist Information Warrants (JIWs)

There were no JIWs issued in the 2020-21 records period.

Table 5- Authorisations issued for telecommunications data on behalf of foreign countries

Agency	Foreign Historic	Foreign Historic Inspected	Foreign Prospective	Foreign Prospective Inspected
AFP	68	**41**	-	**-**

Compliance issues and risks to compliance

This section outlines instances of non-compliance identified across multiple agencies during 2021–22 telecommunications data inspections, and issues that may pose risks to compliance. We will review agencies' actions in response to these issues, and all other findings from the 2021–22 reports, at future inspections.

Our inspections revealed several key areas that we consider pose the greatest risk to an agency's compliance with the Act. These included:

- access to data where the relevant offence thresholds were not met
- insufficient information to demonstrate authorised officer considerations
- inconsistent or inadequate vetting and quality assurance processes to check data received from telecommunications providers
- inconsistent or inadequate agency controls and procedures to ensure officers consider whether a JIW may need to be sought
- inconsistent or inadequate record-keeping about use and disclosure of data received under a telecommunications data authorisation
- gaps in agency training and guidance material
- authorisations for access to telecommunications data being made for purposes not provided for in the Act, and
- discrepancies in agencies' annual reporting on the use of telecommunications data powers to the responsible Minister (currently the Attorney-General).

Access to data where relevant offence thresholds were not met

We found one agency made prospective authorisations for offences that did not meet the threshold during our 2021–22 inspection period. Under s 180(4) of the Act, an authorised officer must not make a prospective authorisation unless satisfied the disclosure is reasonably necessary for the investigation of a serious offence (as defined by s 5D of the Act) or an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.

Prospective authorisations made where offence thresholds were not met

During our inspection at Victoria Police, we identified 451 prospective authorisations made for offences that did not meet the offence thresholds. We identified a further 3 prospective authorisations made with reference to offences under repealed Acts, that would not have met the offence thresholds were the Acts still in force.

We also identified 19 prospective authorisations made for Location Based Services (LBS) where the listed offence was 'missing person'. Under the Act, prospective authorisations cannot be made in relation to locating missing persons. We considered the authorisations identified above were not properly made and, consequently, the information accessed was unauthorised.

We recommended Victoria Police review the records identified by our Office as problematic and quarantine data received for authorisations not meeting legislative thresholds. We recommended Victoria Police seek legal advice on the implications of any use and disclosure of this information and take appropriate remedial action.

In response to our recommendation, Victoria Police advised that legal advice had been obtained and a project team established to work through the relevant authorisations and take actions required to address any issues stemming from use or disclosure of the information accessed under those authorisations. We will review Victoria Police's progress at our next inspection.

Demonstrating authorised officer considerations

There are several key safeguards in the legislation the authorised officer must demonstrate they have considered when making an authorisation. These include:

- weighing the proportionality of the intrusion into privacy against the gravity of the conduct, the value of the information sought and its likely assistance to with enforcing the criminal law, locating a missing person or enforcing a law imposing a pecuniary penalty or protection of public revenue
- ensuring the request is not seeking disclosure of the contents or substance of a communication
- whether a purpose of the telecommunications data disclosure is to identify a journalist's source and, if so, whether a JIW is in force or should be sought
- the authorisation is for a purpose permitted under Chapter 4 and, where applicable, that the relevant offence thresholds are met.

Section 186A(1)(a)(i) of the Act requires that records are kept for each authorisation made that indicate whether the authorisation was properly made. The Ombudsman's view is this includes records of the above considerations.

In reviewing agencies' use of telecommunications data powers, we assess whether the authorised officer had sufficient information to consider the required matters set out in the Act, including privacy considerations under s 180F of the Act, JIW considerations under s 180H of the Act, and whether the relevant purpose and offence thresholds were met from ss 178 to 180Bof the Act.

Without sufficient background information in the request, we do not consider template wording in an authorisation sufficient to demonstrate the authorised officer had turned their mind to the required considerations. While we understand that authorised officers may be aware of background information relating to a particular investigation, we rely on agency record-keeping practices, including the contemporaneous records by authorised officers, to be satisfied the relevant considerations were made.

We made 3 recommendations, 12 suggestions and 14 better practice suggestions across 14 agencies[13] during our 2021–22 inspections aimed at improving agencies' ability to demonstrate authorised officer considerations. These included:

- Increasing the awareness among requesting and authorised officers of the key considerations and record-keeping requirements of the Act
- Implementing measures to ensure requesting and authorised officers consistently document any information, including information from oral briefings, to demonstrate all relevant matters and safeguards were considered before making an authorisation
- Ensuring authorised officers demonstrate they accessed and considered relevant information to fulfil their role as decision-makers, including information the authorised officer must consider to satisfy themselves that the legislative considerations under Chapter 4 of the Act are met.
- Incorporating direct guidance in agencies' standard operating procedures and training about the record-keeping obligations for authorised officers.
- Establishing quality assurance measures to assess requests made for the disclosure of telecommunications data to ensure each request contains sufficient information for an authorised officer to demonstrate they have made the considerations required under Chapter 4 of the Act.

Improving the considerations made by Authorised Officers

During our 2020-21 inspection of the Independent Broad-based Anti-Corruption Commission (IBAC) our Office identified numerous instances of authorised officers not demonstrating that they had consider the requirements under Chapter 4 of the Act prior to making their authorisation. This included not capturing the details from verbal briefings from the requesting officer in the authorisation, failing to demonstrate the relevance of the telecommunication data (including the person of interest or telecommunication service) being sought to the investigation or enforcement of the criminal law, and insufficient information being provided to authorising officer to consider the impact on privacy. We suggested IBAC ensure sufficient information is provided to an authorised officer to enable them to make the necessary privacy considerations, including how the person of interest and service is connected to the investigation.

Following our inspection, IBAC advised they were reviewing their guidance material to requesting officers with a view to updating the content based on our findings and suggestion. IBAC also committed to conducting information sessions with requesting and authorising officers throughout 2021 on the need for authorised officers to record their considerations. The agency was also implementing system changes to

[13] ACLEI, ACIC, AFP, CCC WA, CCC QLD, Home Affairs, NSW CC, NSW Police, NT Police, QPS, SA Police, Tasmania Police, Victoria Police, and WA Police.

making these considerations a mandatory field for authorised officers to complete when making an authorisation.

During our 2021-22 inspection, we were pleased with the progress made by IBAC to address our findings and mitigate any future risks of non-compliance.
We acknowledged IBAC's compliance team had commenced internal audits of the agency's use of telecommunications data to identify compliance issues, improving feedback to requesting or authorising officers to improve decision making and mitigate compliance risks. IBAC's updated telecommunications data training packages were comprehensive and reflected the requirements of the Act and our Office's expectations of best practice.

We made no findings in relation to IBAC's ability to demonstrate authorised officer considerations and were satisfied our previous suggestion and better practice suggestion had been fully implemented.

Data vetting and quality control frameworks

Telecommunications providers sometimes give agencies telecommunications data that was not authorised for disclosure. This is usually inadvertent or due to a provider misunderstanding the terms of the authorisation. We refer to this as 'data outside the parameters of an authorisation'. While agencies may receive data outside the parameters of an authorisation through no fault of their own, agencies are responsible for ensuring this unauthorised data is managed appropriately. Any telecommunications data received outside the parameters of an authorisation should be quarantined from further use or disclosure.

Data vetting involves agencies assessing the information and/or documents received from a provider against what was authorised to ensure the agency is only dealing with data that was authorised.[14] If agencies do not identify data outside the parameters of an authorisation through vetting, this data may be used or disclosed without proper authority. Agencies with insufficient or no consistent data vetting procedures tend to have a higher rate of compliance issues related to managing data outside the parameters of an authorisation. Our Office considers it essential that agencies have formal processes, policies, and training in place for identifying and managing unauthorised telecommunications data.

During our 2021–22 inspections, we found that most agencies received data outside the parameters of an authorisation. While most agencies exercised some form of quality assurance (QA) checks, for many agencies these are ad hoc and depend on

[14] See Appendix A for further information about how we assess whether telecommunications data disclosed by the provider, and used by the agency, complies with the authorisation.

particular individuals taking the initiative to check, rather than having formalised QA processes with structured guidance for vetting incoming telecommunications data.

We made 13 suggestions and 12 better practice suggestions regarding data vetting and quality assurance processes across 11 agencies.[15] These ranged from establishing comprehensive and consistent procedures, formalising existing practices in policy and guidance material, strengthening existing processes or address process gaps, and limiting access to quarantined data.

Identifying and managing unauthorised data vetting and quarantining practices

Our 2020-21 inspection of SA Police found the agency did not have a standardised policy or procedures for vetting telecommunications data returned by telecommunications providers to ensure it was within the parameters of the authorisation.

During our 2021–22 inspection, we found SA Police had not yet implemented a standard vetting procedure or consistent practices for managing unauthorised data. We reiterated our previous suggestion that SA Police should establish standardised policies and procedures for vetting telecommunications data to ensure all data it receives is checked against the parameters of the associated authorisation. We also suggested SA Police should establish standardised procedures for quarantining of telecommunications data received outside the parameters of an authorisation. Such procedures should ensure SA Police can:

- clearly identify in all related systems and registers those records that are subject to quarantining
- securely store quarantined telecommunications data in an appropriate location with minimal accessibility
- ensure any copies disseminated to investigators or external agencies are deleted or destroyed, and records maintained to demonstrate this has occurred.

In response, SA Police advised it has enhanced data vetting processes and finalised training packages, with substantial improvement initiatives underway to address all reported inspection findings.

Journalist Information Warrant (JIW) controls

The requirement to obtain a JIW was introduced by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*. If an agency wishes to access the telecommunications data of a person working as a journalist or their

[15] ACLEI, ACCC, ACIC, CCC QLD, CCC WA, NSW Police, QPS, SA Police, Tasmania Police, Victoria Police, WA Police.

employer, and a purpose is to identify a journalist's source, the agency must apply to an external issuing authority for a JIW before it can make a telecommunications data authorisation. The JIW regime recognises the public interest in protecting journalists' sources while ensuring agencies have the investigative tools necessary to protect the community.

To demonstrate the authorised officer gave due consideration to the requirements of the Act, we consider agencies should have appropriate procedures and controls so an authorised officer can:

- identify the circumstances where a JIW may be required
- record their considerations, including where legal or other advice was sought to help in their decision-making.

Given the complexity of the legislative tests that apply to potential journalist involvement and JIW requirements, we consider it better practice for authorised officers to seek guidance where a journalist may be involved.

During our inspections we review an agency's JIW processes and controls, including:

- policies and procedures, 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.

We did not identify any telecommunications data authorisations in fact issued without a journalist information warrant, when such a warrant was required. Nevertheless, due to the importance of JIWs as safeguards, during our 2021–22 inspections, we made 7 suggestions and 15 better practice suggestions across 15 agencies on improving controls agencies had in place to ensure JIW requirements are met.[16] While many agencies were aware of the JIW requirements, we identified several gaps in guidance and templates including:

- A lack of in-built controls in requesting and authorising processes to require officers to turn their minds to whether requests related to a journalist or an employer of journalists, and if the request was to gather information in relation to a source
- Inconsistent advice to requesting and authorising officers regarding JIW requirements.
- Ensuring policy, procedures templates and training materials are consistent with s 180H of the Act.

[16] ACLEI, ACIC, AFP, ACCC, CCC QLD, Home Affairs, ICAC SA, LECC, NSW CC, NSW Police, NT Police, SA Police, Tasmania Police, Victoria Police and WA Police.

Our view is that requesting and authorised officers should actively turn their mind to whether a purpose of making any telecommunications data request is to identify a possible source of a journalist or a journalist's employer.

Insufficient guidance for staff on JIW considerations

Our 2020–21 inspection of ACLEI identified insufficient controls in place to ensure authorised officers consider whether JIW provisions could apply before making an authorisation under Chapter 4 of the Act. We suggested ACLEI incorporate direct guidance within its standard operating procedures on the steps to be taken where a request may relate to a journalist. We also suggested ACLEI update its template to ensure it includes guidance on engaging with the ACLEI's legal team where a journalist may be involved, before any further actions are undertaken.

During our 2021–22 inspection, we noted ACLEI had updated its templates and procedures to include material relating to JIW considerations. However, we found this guidance was inconsistent with relevant provisions under Chapter 4 of the Act, creating ambiguity when requesting and making telecommunication data authorisations. This guidance also did not encourage requesting and authorising officers to consult with ACLEI's legal team in circumstances where a JIW was potentially required or to document their considerations under s 180H of the Act prior to making an authorisation.

To ensure ACLEI could meet its record-keeping obligations under s 186A(1)(a)(i) of the Act and demonstrate that it has made the relevant considerations in relation to s 180H of the Act, we suggested ACLEI further update its standard operating procedures to prompt engagement with the legal team when a JIW may be required, document authorising officers' JIW considerations and provide guidance on the range of activities that might constitute a journalist or journalistic organisation to assist in considering the need to engage with legal about possible JIW considerations.

In response, ACLEI advised it would adopt our suggestion and amend its standard operating procedures and templates.

Use and disclosure record-keeping obligations

Section 182 of the Act specifies certain circumstances in which telecommunications data accessed under a Chapter 4 authorisation may be used or disclosed and prohibits data to be used or disclosed outside of these circumstances. The Act also specifies record-keeping obligations under s 186A(1)(g)(iii) requiring agencies to keep records that indicate whether any use or disclosure took place in the permitted circumstances.

Our Office assesses whether an agency has processes and documentation in place to account for the use and disclosure of telecommunications data it has accessed under Chapter 4 of the Act. We consider adequate record-keeping fundamental to agencies demonstrating accountable use of telecommunications data access powers under Chapter 4 of the Act.

Across 8 agencies[17] inspected in the 2021–22 inspection period, we made 6 suggestions and 2 better practice suggestions regarding use and disclosure record-keeping obligations. These included:

- developing guidance, policies, procedures and training about the restrictions on use and disclosure of telecommunications data and how to meet related record-keeping obligations
- implementing consistent record-keeping mechanisms for use and disclosure of telecommunications data
- providing reminders and prompts to staff about the obligation to keep records when using or disclosing telecommunications data.

Unable to assess use and disclosure of telecommunications data

Over the previous 2 inspections, we identified that Tasmania Police did not have clear procedures and guidelines for recording use and disclosure of telecommunication data, as required under s 186A(1)(g) of the Act.

During our 2021-22 inspection, Tasmania Police disclosed that telecommunications data stored on its systems is not able to be restricted to individuals or teams, and there was no audit capability to be able to track which individuals have accessed specific records stored through the platform they were using. The primary repository for historic data returned from a carrier, once uploaded, was available to all Tasmania Police members with access to the system.

We also found there were no records to indicate whether Tasmania Police used or disclosed telecommunications data its members have access to. As such, we were unable to determine whether any use and disclosure that occurred was in the circumstances permitted under the Act.

We recognised Tasmania Police is overhauling its governance framework for its use of Chapter 4 powers. We suggested Tasmania Police, as part of enhancing this governance framework, develop procedures and guidelines for recording use and disclosure of telecommunication data. We also suggested Tasmania Police considers options for securely storing telecommunication data to minimise unauthorised access, use and/or disclosure.

[17] ACLEI, AFP, CCC WA, Home Affairs, ICAC SA, SA Police, Victoria Police and WA Police.

In response, Tasmania Police advised they have initiated modifications to their systems to enhance record keeping, including the introduction of limitations on access to telecommunication data and recording of use and disclosure. This is supported by implementing training and guidance to requesting and authorising officers and changing templates to reinforce use and disclosure obligations.

Training and guidance for officers

Deficiencies in practical guidance material (including training) or documented processes and procedures to ensure compliant authorisation of access to telecommunication data contribute to the systemic compliance problems we identify through our inspections. Ensuring officers involved in requesting, authorising, using, and managing telecommunications data are aware of the requirements of the Act supports consistent compliance with the Act, and early remedial action when compliance issues arise. Agencies lacking effective training or guidance experienced greater issues in officers understanding and consistently applying fundamental aspects of the legislation, including maintaining records to demonstrate compliance.

We made 2 recommendations, 5 suggestions, and 1 better practice suggestions across 6 agencies[18] about improving training, guidance and support for officers involved in requesting, authorising, using, and managing telecommunications data.

Lack of centralised policy and guidance for making telecommunications data authorisations

During our 2021-22 inspection, we found that WA Police policy and procedural framework consisted of multiple documents across various business areas using the Chapter 4 powers. Some of the documents required updating and greater clarity of the specific administrative processes to be undertaken by WA Police to ensure compliance with the Act. This included revising and providing consistent advice on:

- vetting and quarantining data results
- authorised officer considerations
- requirements and quality controls for submitting requests to a carrier
- journalist information warrant considerations
- authorisations being written or electronic (not verbal) form
- identifying and logging compliance issues
- managing data and preparing statistics for the Ombudsman and ministerial reports.

We suggested that WA Police update its policies and procedures to include or more clearly define the specific administrative processes to be undertaken by WA Police

[18] AFP, IBAC, NT Police, SA Police, Tasmania Police, and WA Police

to support its compliance with Chapter 4 of the Act. We also made a better practice suggestion for WA Police to consolidating its telecommunications data guidance, particularly on policies and procedures relating to the same legislative power, to facilitate consistency across different business areas.

In response, WA Police advised they had developed a centralised standard operating procedure for telecommunications authorisation and Authorised Officers procedures. The new procedure provided a single point of reference for all areas of WA police accessing and authorising telecommunication data.

Authorisations being made for purposes not provided for in the Act

SS 178(2), 178A(2) 179(2) and 180(2) of the Act identify the purpose with which an authorised officer can access telecommunication data or prospective data. While our Office does not assess the merits of authorisations, we focus on whether the records kept by the agency demonstrate the authorisation was properly made, including:

- specified information or documents to be accessed
- the carrier(s)/carriage service provider(s) from which the information is sought
- the authorised officer's satisfaction that the authorisation was reasonably necessary for a relevant purpose provided for under Chapter 4 of the Act, including meeting the relevant offence threshold
- sufficient information was provided for the authorised officer to appropriately consider the privacy requirements under s 180F of the Act
- does not give rise to any potential disclosure that would require a JIW to be in force.

During our 2021-22 inspections, we found instances of agencies making authorisations for:

- purposes not provided for under the Act
- access to information that is not telecommunications data
- access to information from organisations that are not telecommunications providers

We made 1 recommendation, 14 suggestions and 4 better practice suggestions across 7 agencies[19] in relation to the use of Chapter 4 authorisations for purposes not provided for under the Act.

Using Chapter 4 powers to access non-telecommunication data

During our 2021-22 Inspection of NSW Police Force (NSWPF), we checked records labelled as seeking quotes from providers for provision of telecommunication data,

[19] ACIC, AFP, NSW Police. NT Police, SA Police, Tasmania Police and Victoria Police.

which showed Chapter 4 authorisations and telecommunications data disclosure notifications being sent to telecommunications providers seeking quotes.

We do not consider requests for quotes from carriers to be 'information or documents' covered under ss 276, 277 and 278 of the *Telecommunications Act 1997,* that require authorised access by way of an authorisation under Chapter 4 of the Act. We do not consider it appropriate to use the Chapter 4 authorisation provisions for requesting this information from telecommunications providers.

The incorrect use of Chapter 4 authorisation provisions creates risks for NSWPF in counting non-disclosure actions as s 178 authorisations for statistical reporting purposes under s 186(1) of the Act, leading to ministerial reporting inaccuracies. Further, telecommunications data may be disclosed by a carrier in response to the authorisation, resulting in unauthorised data being passed to NSWPF. We suggested that NSWPF should cease the use Chapter 4 authorisations for purposes not provided for in the Act.

In response, NSWPF acknowledge this finding and were seeking to update their processes to prevent Chapter 4 authorisations being used for requesting quotes from telecommunication providers.

Reporting to the Minister

Section 186 of the Act requires each enforcement agency to give a written annual report to the Minister (currently the Attorney-General). This report is due as soon as practicable (and in any event within 3 months after each 30 June) and must set out the number of historic authorisations made by an authorised officer under sections 178, and 179 of the Act and the number of prospective authorisations made under section 180 of the Act.

Our Office views this reporting obligation as a key accountability measure for agencies' use of telecommunications data powers under Chapter 4 of the Act, supporting transparency to Parliament and the public about the extent of access to telecommunications data by enforcement agencies. We consider it critical that agencies account accurately and completely for their use of Chapter 4 powers.

We made 1 recommendation, 6 suggestions and 2 better practice suggestions across 5 agencies[20] during our 2021–22 inspections in relation to reporting to the Minister.

[20] ACIC, AFP, CCC QLD, LECC, and QPS.

Inaccuracies in annual report

During our 2020–21 inspection at the CCC QLD, we found inaccuracies in the agency's annual report to the Minister. We suggested the CCC QLD issue and addendum to the Minister to correct the reporting errors and implement quality control measures to ensure that reporting to the Minister on the use of telecommunications data powers is accurate.

While the CCC QLD advised that sufficient measures were in place, during our 2021–22 inspection we identified telecommunications data authorisations that had not been included in the 2020–21 annual report to the Minister (now the Commonwealth Attorney-General). This reporting discrepancy largely occurred due to instances where:

- records were not completed in full
- the date of completion was recorded after 30 June 2021 and
- the authorisation was not registered in the system.

We suggested the CCC QLD:

- revise its reporting methodology to ensure it is capturing the authorisations made during the reporting period
- implement effective quality control measures to ensure that its annual reporting to the Minister on the use of telecommunications data powers is accurate
- review its reporting for the periods 2018-19, 2019-20 and 2020-21 to confirm reporting accuracy and issue an addendum to the Minister for the relevant periods, where required.

In response, the CCC QLD noted it has revised its reporting methodology to ensure that future annual reports to the Minister will show the number of authorisations made in the relevant period. Further, the CCC QLD had noted that checks will be made at the end of each month to confirm the required details have been entered into the agency's database.

The CCC QLD advised it had also reviewed its reporting information for 2018/19, 2019/20 and 2020/21 and has provided addendums containing the correct statistics to the Minister.

Appendix A - How we assess that telecommunications data disclosed by the telecommunications provider, and used by the agency, complies with the authorisation

In some instances, telecommunications providers may provide additional information that an agency did not specifically authorise. As discussed above in 'Data vetting and quality control frameworks', when this occurs, we expect an agency to identify and quarantine the data from any use or disclosure.

We undertake our own assessments of the data received by an agency during inspections and confirm it:

- is within the parameters of an authorisation, including for the correct service number and within the relevant timeframe specified on an authorisation.
- is the type of data that has been 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	1234567
Authorised data	Call charge records
Period authorised	1/07/2018 to 30/06/2019
Date/time 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)	1234567	8910012
2	01/07/2018 0300 (UTC)	1234567	8910012
3	01/07/2018 0900 (UTC)	8910012	1234567
…			
10	30/06/2019 0359 (UTC)	1234567	8910012
11	30/06/2019 0500 (UTC)	1234567	8910012

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, not calls received by this number.
10	This line is authorised, as after conversion to AEST, it occurred at 30/06/2019 1359, being before the time the authorisation was notified to the carrier.
11	This line is not authorised, as after conversion to AEST, it occurred at 30/06/2019 1500, being after the time the authorisation was notified to the carrier.
For these results, we would expect the agency to proactively identify and quarantine the unauthorised data (lines 3 and 11) before results were disseminated to an investigator. Where this unauthorised information is not identified before dissemination, we suggest the agency contacts any recipients to ensure the data is quarantined. We also suggest the agency ascertain whether use or disclosure took place and if so, seek legal advice.	

Appendix B – 2021–22 stored communications and telecommunications data inspection schedule

Agency	Inspection type	Inspection Start Date	Inspection Finish Date
QPS	Stored Communications	26-Jul-2021	30-Jul-2021
ACLEI	Telecommunications Data	26-Jul-2021	30-Jul-2021
ASIC	Telecommunications Data	2-Aug-2021	5-Aug-2021
ACIC	Stored Communications	23-Aug-2021	26-Aug-2021
CCC QLD	Telecommunications Data	30-Aug-2021	3-Sep-2021
WA Police	Telecommunications Data	30-Aug-2021	3-Sep-2021
ACCC	Stored Communications & Telecommunications Data	20-Sep-2021	23-Sep-2021
Home Affairs	Stored Communications & Telecommunications Data	27-Sep-2021	1-Oct-2021
LECC	Stored Communications & Telecommunications Data	11-Oct-2021	15-Oct-2021
ICAC SA	Stored Communications & Telecommunications Data	19-Oct-2021	21-Oct-2021
CCC QLD	Stored Communications	19-Oct-2021	22-Oct-2021
CCC WA	Telecommunications Data	26-Oct-2021	29-Oct-2021
ACIC	Telecommunications Data	8-Nov-2021	12-Nov-2021
WA Police	Stored Communications	9-Nov-2021	12-Nov-2021
ICAC NSW	Stored Communications & Telecommunications Data	16-Nov-2021	18-Nov-2021
AFP	Stored Communications	22-Nov-2021	26-Nov-2021
NSW CC	Stored Communications & Telecommunications Data	29-Nov-2021	2-Dec-2021
VIC Police	Telecommunications Data	29-Nov-2021	3 Dec-2021
NSW Police Force	Telecommunications Data	17-Jan-2022	21-Jan-2022
AFP	Telecommunications Data	30-Jan-2022	11-Feb-2022
NSW CS	Health check- Telecommunications Data	22-Feb-2022	24-Feb-2022
IBAC	Telecommunications Data	28-Feb-2022	3-Mar-2022
NT Police	Stored Communications & Telecommunications Data	7-Mar-2022	11-Mar-2022
ACLEI	Stored Communications	15-Mar-2022	17-Mar-2022
QPS	Telecommunications Data	4-Apr-2022	6-Apr-2022
VIC Police	Stored Communications	23-May-2022	27-May-2022
SA Police	Telecommunications Data	30-May-2022	3-Jun-2022
NSW Police Force	Stored Communications	6-Jun-2022	10-Jun-2022
TAS Police	Stored Communications & Telecommunications Data	27-Jun-2022	1-Jul-2022

Appendix C – Stored communications inspection criteria 2021–22

Objective: To determine the extent of compliance with Chapter 3 of the *Telecommunications (Interception and Access) Act 1979* (the Act) by the agency

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

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

Process checks:

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

Records checks in the following areas:
Domestic preservation notices:

- Whether the agency could give the type of domestic preservation notice given (s 107J(1)(a) of the Act)?
- Whether the domestic preservation notice only requested preservation for a period permitted by s 107H(1)(b) of the Act?
- Whether the domestic preservation notice only related to one person and/or one or more services (s 107H(3) of the Act)?
- Whether the relevant conditions for giving a domestic preservation notice were met (s 107J(1) of the Act)?
- Whether the domestic preservation notice was given by a person with the authority to do so (s 107M of the Act)?

Foreign preservation notices:

- Whether the foreign preservation notice only requested preservation for a permitted period (s 107N(1)(b) of the Act)?
- Whether the foreign preservation notice only related to one person and/or one or more services (s 107N(2) of the Act)?
- Whether the relevant conditions for giving a foreign preservation notice were met (s 107P of the Act)?
- Whether the foreign preservation notice was given by a person with the authority to do so (s 107S of the Act)?

1.2 Did the agency revoke preservation notices when required?

Process checks:

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

Records checks in the following areas:
Domestic preservation notices:

- Whether the domestic preservation notice was revoked in the relevant circumstances (s 107L of the Act)?
- Whether the domestic preservation notice was revoked by a person with the authority to do so (s 107M of the Act)?

Foreign preservation notices:

- Whether the foreign preservation notice was revoked in the relevant circumstances (s 107R of the Act)?
- Whether the foreign preservation notice was revoked by a person with the authority to do so (s 107S of the Act)?

2. Is the agency only dealing with lawfully accessed stored communications?

2.1 Were stored communications properly applied for?

Process checks:

- Does the agency have procedures in place to ensure that warrants are in the prescribed form (s 118(1) of the Act)?

Records checks in the following areas:

- Whether the warrant was applied for by a person with the authority to do so (s 110(2) of the Act)?
- Whether applications for stored communications warrants were made in accordance with ss 111 to 113 of the Act, or ss 111(2), 114 and 120(2) of the Act for telephone applications?
- Whether the facts and other grounds in the application made by the agency provided accurate and sufficient information for the issuing authority to make a fully informed decision (ss 113(2) and 116 of the Act)?
- Whether the application was only in relation to one person (s 110(1) of the Act)?
- If a warrant relates to the same person and the same telecommunications service as a previous warrant – whether the warrant was issued in accordance with s 119(5) of the Act?
- Whether a connection can be established between the person listed on the warrant and the relevant telecommunications service (s 117 of the Act)?

2.2 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 of the Act?

2.3 Did the agency revoke stored communications warrants when required?

Process checks:

- Where an agency becomes aware that the grounds on which a stored communications warrant was issued have ceased to exist, does the agency have processes in place to seek revocation of the warrant (s 122 of the Act)?

3. Has the agency properly received and managed accessed stored communications?

3.1 Were stored communications properly received by the agency?

Process checks:

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

Records checks in the following areas:

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

3.2 Did the agency appropriately deal with accessed stored communications?

Process Checks:

- Does the agency have processes in place to accurately identify and manage any stored communications received outside the parameters of a warrant or accessed by the carrier after the warrant ceased to be in force?
- Does the agency have controls, guidance and/or training in place around dealing with stored communications?

Records checks in the following areas:

- Did the agency identify any stored communications received that did not appear to have been lawfully accessed?
- Did the agency quarantine stored communications that did not appear to have been lawfully accessed?
- Whether any use, communication or recording of lawfully accessed information has been accounted for in accordance with ss 139 – 146 of the Act?

3.3 Were stored communications properly dealt with and destroyed?

Process checks:

- Does the agency have procedures in place for the destruction of stored communications, and are they sufficient?

Records checks in the following areas:

- Whether accessed stored communications were destroyed in accordance with s 150(1) of the Act?

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

Process checks:

- Does the agency have processes in place which enable it to accurately report to the Minister on the number of preservation notices given and warrants issued (s 159 of the Act)?
- Did the agency have effective record-keeping practices in place (including keeping records regarding any use, communication or recording of lawfully accessed information)?

Records checks in the following areas:

- Whether the chief officer provided the Minister a written report, within three months after 30 June, that sets out the extent to which information and records were destroyed in accordance with s 150 of the Act (s 150(2) of the Act)?
- Whether the agency has kept records in accordance with s 151 of the Act?
- Whether the chief officer has provided an annual report to the Minister, within three months after 30 June, regarding applications and warrants (s 159 of the Act)?

5. Does the agency have a culture of compliance?

- Is there a culture of compliance?
- Does the agency undertake regular training for officers exercising powers?
- Does the agency provide support and appropriate guidance material for officers exercising powers?
- Was the agency proactive in identifying compliance issues?
- Did the agency disclose compliance issues to the Commonwealth Ombudsman's office?
- Were issues identified at previous inspections addressed?
- Has the agency engaged with the Commonwealth Ombudsman's office, as necessary?

Appendix D – Telecommunications data inspection criteria 2021–22

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

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

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

Process checks

- 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 training in place for requesting and processing officers to ensure they have sufficient understanding of compliance obligations?
- Does the agency have effective controls, guidance and training in place for authorised officers to ensure that authorisations are properly given?
- Does the agency have effective procedures in place to identify when prospective authorisations are no longer required and should be revoked, and to notify carriers of any revocations?

Records checks in the following areas

- Whether authorisations were in written or electronic form as required by the Act
- Whether authorisations, notifications and revocations complied with the form and content requirements as determined by the Communications Access Coordinator (s 183(1)(f)) of the Act
- Whether there is evidence of sufficient information before an authorised officer, prior to them making an authorisation, to enable them to properly consider the matters listed in s 180F of the Act
- Whether authorisations were only made for information permitted by the Act, with consideration to s 172 of the Act
- Whether authorised officers have demonstrated that they have considered matters listed under s 180F of the Act, and are satisfied, on reasonable grounds, that the privacy interference is justified and proportionate
- Whether authorisations were made by officers authorised under s 5AB of the Act
- Whether authorisations were made in relation to specified information or documents (ss 178 to 180 of the Act)
- Whether prospective authorisations are in force only for a period permitted by s 180(6) of the Act
- Whether prospective authorisations were revoked in relevant circumstances (s 180(7) of the Act)

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

Process checks

- Does the agency have effective and consistent procedures in place to screen and quarantine telecommunications data it obtains?

Records 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 quarantined the data from use (and if appropriate, sought clarification from the carrier)

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

Process checks

- Does the AFP have effective procedures in place to ensure that foreign authorisations are properly applied for, given, extended and revoked, and are they sufficient?
- Did the AFP ensure that foreign authorisations were only made in relation to permitted information that was not content?

Records checks in the following areas

- Whether authorisations for telecommunications data on behalf of a foreign law enforcement agency were properly given and disclosed (ss 180A to 180E of the Act)
- Whether the Attorney-General made an authorisation before a prospective authorisation was made under s 180B of the Act
- Whether foreign prospective authorisations were properly revoked in accordance with s 180B(4) of the Act
- Whether extensions of foreign prospective authorisations were properly made in accordance with ss 180B(6) and (7) of the Act

2. Has the agency properly managed telecommunications data?

Process checks

- Does the agency have secure storage facilities for telecommunications data and associated information?
- Does the agency have procedures in place to limit access to telecommunications data that it has obtained?
- Does the agency have processes in place to account for the use and disclosure (and secondary use and disclosure) of telecommunications data?

Records checks in the following areas

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

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

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

Process checks

- Does the agency have effective procedures and controls in place to identify the circumstances where a journalist information warrant may be required?

Records checks in the following areas

- Whether officers of the agency actively turned their minds to whether a request related to a journalist

- Whether officers of the agency kept sufficient records around a determination as to whether a request related to a journalist

3.2 Did the agency properly apply for journalist information warrants?

Process checks

- Does the agency have effective procedures and controls in place to ensure that a journalist information warrant is sought in every instance where one is required (s 180H) of the Act?
- Does the agency have effective procedures in place to ensure that journalist information warrants are properly applied for and issued in the prescribed form?

Records checks in the following areas

- Whether the application was made to a Part 4-1 issuing authority (s 180Q(1) of the Act)
- Whether the application related to a particular person (s 180Q(1) of the Act)
- Whether the application was made by a person listed under s 180Q(2) of the Act
- Whether the warrant was issued for a permitted purpose by s 180U(3) of the Act
- Whether the warrant was in the prescribed form and signed by the issuing authority (s 180U(1) of the Act)

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

Records checks in the following areas

- Whether the Ombudsman was given a copy of each warrant issued to the agency as soon as practicable (s 185D(5) of the Act)
- Whether the Ombudsman was given a copy of each authorisation given under the authority of a journalist information warrant, as soon as practicable after the expiry of that warrant (s 185D(6) of the Act)

3.4 Did the agency revoke journalist information warrants when required?

Process checks

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

Records checks in the following areas

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

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

Process checks

- Does the agency have processes in place which enable it to accurately report to the Minister on the number of authorisations made and journalist information warrants issued, as well as all other matters listed under s 186 of the Act?
- Does the agency have effective record-keeping practices in place?
- Does the agency have effective record-keeping practices that sufficiently demonstrate compliance, including:
    - Records demonstrating an authorised officer's considerations of the matters listed ins 180F of the Act

- Records to demonstrate compliant use and disclosure (and secondary use and disclosure)

Records checks in the following areas

- Whether the agency sent an annual report to the Minister on time, in accordance with s 186 of the Act and whether the report accurately reflected the agency's use of the Chapter 4 powers
- Whether the agency has kept records in accordance with s 186A of the Act
- Whether the agency retains all other relevant records to enable our Office to determine compliance, this may include training and guidance documents that are provided to requesting and authorising officers, records of data received or quarantined and file notes addressing discrepancies.

5. Does the agency have a culture of compliance?

Process checks

- Is there a culture of compliance?
- Does the agency undertake regular training for officers exercising Chapter 4 powers?
- Does the agency provide support and appropriate guidance material for officers exercising Chapter 4 powers?
- Was the agency proactive in identifying compliance issues?
- Did the agency disclose compliance issues to the Commonwealth Ombudsman's office?
- Were issues identified at previous inspections addressed?
- Has the agency engaged with the Commonwealth Ombudsman's office, as necessary?
- Does the agency have processes to ensure compliance, including:
  - Quality control processes are supported by policy and practical guidance documents?
  - Effective procedures to measure compliance and identify and action issues as they arise?
  - Processes and training to identify and track issues that occur?
  - Protocols for advising relevant officers of issues that arise?

Appendix E – Telecommunications data 'health check' inspection criteria 2021–22

Objective: To assess the 'health' of the agency in establishing its compliance framework and to determine any current or future compliance risks with Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (the Act)

The 'health check' will assess the readiness of the agency's compliance framework against the criteria below, which is informed by the Australian Standard on Compliance Management Systems – Guidelines (AS ISO 19600:2015)

1. Compliance preparedness

1.1 Organisational context

- Has the agency identified any external and internal issues, especially those related to compliance risks, that affect its ability to establish processes for, and perform, the powers under Chapter 4 of the Act?
- Does the agency have a clear framework of policies and procedures that supports compliance with legislative obligations that arise from the powers under Chapter 4 of the Act?
    - Has this framework been communicated to staff who exercise or are involved in exercising the powers under Chapter 4 of the Act?

1.2 Compliance culture

- Does the agency demonstrate a consistent and sustained commitment by management (at all levels) towards effective compliance behaviours throughout the agency?
- Do senior management demonstrate their leadership and commitment with respect to the agency meeting its compliance obligations?
- What are the messages conveyed to staff about compliance and expectations, generally and specifically in regard to exercising powers under Chapter 4 of the Act?
- What actions are taken by leadership to support effective compliance?

1.3 Compliance policy

- Does the agency have a documented compliance policy (or equivalent)?
    - What does a compliance policy document look like?
- How is this policy document communicated/made available within the agency?
    - Specifically, how is it communicated to the officers with responsibilities under Chapter 4 of the Act?
- When was the compliance policy last updated?

1.4 Actions to address compliance risks

- Does the agency have a risk register and risk management plan regarding compliance with Chapter 4 of the Act?
- Has the agency sought legal review of its policies and procedures for the use of the powers under Chapter 4 of the Act and management of information received under Chapter 4 authorisations?

- This will ensure its processes and systems are compliant with the Act and mitigate risk of non-compliance.

1.5 Compliance objectives and planning to achieve them

- Has the agency established plans to ensure compliance with legal requirements in exercising the agency function?
- What are the outstanding actions, if any, to establish compliance plans and anticipated timeframes for implementation?

1.6 Organisational roles, responsibilities and authorities

Delegations

- Is there a delegation instrument (or multiple instruments) in place for the purposes of s 5AB of the Act?
- Do the delegations reflect the current organisational structure?
- Are only officers at an appropriate level delegated?
- How are officers made aware of the delegation instrument?
- If the delegation instrument is position based, do the current procedures include mitigations for the potential risks associated with organisational change? (staff leaving and joining the agency)

Authorised officers

- Are the chief officer and the delegates made sufficiently aware of their obligations regarding authorisations under Chapter 4 of the Act?

2. Support, training and guidance

2.1 Resources

- Has the agency developed a support, training and guidance framework to implement its function?
- What documentation has been, or will be, established by the agency to support its compliance with the Chapter 4 of the Act?
- Has the agency identified and set up the necessary resources to manage its function?
- If resources are currently in development, what are the outstanding actions and anticipated timeframes for completion?

2.2 Competence and training

- Does the agency (or does the agency have an established plan to):
  - hold mandatory and periodic refresher training for officers delegated to exercise the agency's function?
  - engage with the agency delegates to advise on relevant issues/compliance concerns?
- If not established, what are the outstanding actions to establish a training plan and anticipated timeframes for implementation?

2.3 Awareness and communication

- How will the agency ensure that the agency delegates maintain awareness of their roles and compliance responsibilities?

- How will the agency adequately communicate with relevant external stakeholders about its role and functions, and their development?

3. Operational preparedness

3.1 Operational planning

Applying for TD authorisations

- Does the agency have in place policies, procedures and templates for applying for and authorising authorisations in accordance with Chapter 4 of the Act?
- Is the guidance available accurate, comprehensive, practical and efficient?
    - Are the responsibilities of both requesting and authorised officers covered?
- Does the agency's procedural and guidance documentation include:
    - the limitations applicable to the agency's status as an 'enforcement agency' (as opposed to a 'criminal law enforcement agency')?

Journalist Information Warrants (JIWs)

- If applicable - Does the agency have in place policies, procedures and templates for applying for JIWs under s 180Q of the Act?
- Does the agency's procedural and guidance documentation include:
    - The s 180H of the TIA Act restriction that:
    - An authorised officer of an enforcement agency must not (unless JIW in place) make an authorisation under section 178, 178A, 179 or 180 (not applicable for enforcement agency) that would authorise the disclosure of information or documents relating to a particular person if:

        (a) the authorised officer knows or reasonably believes that particular person to be:

            (i) a person who is working in a professional capacity as a journalist; or

            (ii) an employer of such a person; and

        (b) a purpose of making the authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source.

Cancelling or revoking authorisations – *No revocation requirement for historic authorisations*

- Has the agency established policies, procedures and templates for cancelling historic authorisations in accordance with Chapter 4 of the Act?
- Has the agency established policies, procedures and templates for processing the revocation of prospective authorisations in accordance with Chapter 4 of the Act?

Record-keeping

- Has the agency established policies and procedures for its reporting and record-keeping requirements under Chapter 4 of the Act?
    - Such as annual reporting to the minister, use and disclosure logs?
- Has the agency established policies, procedures and templates for issuing evidentiary certificates in accordance with Chapter 4 of the Act (ss 185A, 185C)?
- Has the agency established policies and procedures to store and manage protected information and ensure protected information is not used, recorded, disclosed or admitted in evidence unless an exception applies under Chapter 4 of the Act?
- Has the agency established policies and procedures for facilitating Ombudsman inspections under Chapter 4A of the Act?

- Are the relevant standard operating procedures available to everyone involved in the exercise of the powers under Chapter 4 of the Act?
- Where the above policies and procedures are not yet established, what are the outstanding actions and anticipated timeframes for implementation?

3.2 Establishing controls and procedures

- Does the agency have quality assurance and control measures established for exercising its powers under Chapter 4 of the Act?
- If applicable, has the agency established data management procedures (including vetting and quarantining when required) for electronic information received directly from the carriers?
- Where quality assurance and control measures are not yet established, what are the outstanding actions and anticipated timeframes for implementation?

4. Performance evaluation and improvement

4.1 Monitoring, measurements, analysis and evaluation

- Does the agency have systems in place for capturing and responding to internal and external feedback on the agency's compliance performance, including:
    - staff feedback
    - carrier/provider feedback
    - other stakeholder feedback
- How will the agency identify and manage emerging compliance issues?

4.2 Non-compliance identification and corrective action

- Does the agency have systems and processes in place to identify and respond to compliance issues?

4.3 Audit and management review

Internal review

- Does the agency conduct, or intend to conduct, any form of internal audit or routine review of the agency's compliance with Chapter 4 of the Act?

4.4 Continual improvement

- Does the agency have systems and processes in place to facilitate continual improvement of its administration of its powers under Chapter 4 of the Act?

Appendix F – Glossary of terms

Term (and section of the Act)	Description
The Act	Telecommunications *(Interception and Access) Act 1979*
AAT	Administrative Appeals Tribunal
Accessing a stored communication s 6AA	For the purpose of the 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 Act	Under the Administrative Arrangements Order made on 1 June 2022, commencing 1 July 2022, the Attorney-General is now responsible for the administration of the Act, except to the extent it is administered by the Minister for Home Affairs in relation to the Australian Security Intelligence Organisation.
Administrative errors	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.
Officers approved to exercise the authority of stored communications warrants s 127	Under s 127(1) of the Act the authority conferred by a stored communications warrant may only be exercised by a person in relation to whom an approval under s 127(2) is in force in relation to the 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 specified 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 or carriage service provider to enforcement agencies. *Historic authorisation*s Agencies may authorise the disclosure of specified information or documents that came into existence before a carrier or carriage

Term (and section of the Act)	Description
	service provider 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 offence against any Australian law that is punishable by imprisonment for at least 3 years. Prospective authorisations come into force at the time the carrier or carriage service provider 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 JIWs 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 or carriage service provider 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. 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*

Term (and section of the Act)	Description
	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	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, however described by each specific 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 2018* The above determinations were made under subsection 183(2) of the Act which specifies that the Communications Access Co-ordinator may, by legislative instrument, determine requirements of the form of authorisations, notifications and revocations relating to telecommunications data.
Criminal law enforcement agency s 110A	Section 110A of the 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.

Term (and section of the Act)	Description
	Where an agency does not have a strict timeframe for destructions, in assessing compliance with this provision, our Office makes an assessment based on our understanding of an agency's policies and procedures and what we consider to be reasonable in the circumstances.
Disclosure by agencies to our Office	Prior to or during an inspection, agencies may make a disclosure to our Office outlining one or more 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 should fall within the parameters specified in the authorisation.
Exit interview	Following an inspection, we hold an exit interview with officers of the agency. We present our preliminary inspection and give the agency 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 times 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, streamlined or findings letter.

Term (and section of the Act)	Description
	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 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 ss 180H, 180R-T and 180X	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 to an eligible Judge, Magistrate or AAT 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 s 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.

Term (and section of the Act)	Description
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	For the period to which this report relates, the Minister for Home Affairs was the relevant minister. Under the Administrative Arrangements Order made on 1 June 2022, commencing 1 July 2022, the Attorney-General is now the relevant minster, except in relation to the Australian Security Intelligence Organisation where the relevant minister is 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 (of authorisation) 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.
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 forms s 118(1)(a) s 180U(1)	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*. A journalist information warrant must be in the prescribed form. The prescribed form of a journalist information warrant is set by Form 7 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.

Term (and section of the Act)	Description
	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 the end of the 29th day after receipt. <u>Foreign preservation notices</u> • If the AFP 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 AFP 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 that matters relating to privacy must be considered by an authorised officer before making a telecommunications data authorisation.
	
	The authorised officer considering making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate having regard to the following matters:
	• the gravity of any conduct in relation to which the authorisation is sought, including:
	  ○ the seriousness of any offence in relation to which the authorisation is sought
	  ○ the seriousness of any pecuniary penalty in relation to which the authorisation is sought
	  ○ the seriousness of any protection of the public revenue in relation to which the authorisation is sought

Term (and section of the Act)	Description
	○ 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 JIW, 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

Term (and section of the Act)	Description
	• Other actions in line with agency policies and procedures.
Receiving stored communications information s 135	Section 135(2) of the Act states the chief officer of a criminal law-enforcement agency may authorise in writing officers or classes of officers, of the agency to receive information obtained by accessing stored communications under stored communications warrants, or classes of such 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 we may make a recommendation 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, for example the serious offence, or missing person or pecuniary penalty involved • 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 2020–21 financial year we primarily reviewed records for the 2019–20 financial year.
Revocation ss 107J, 107L, 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

Term (and section of the Act)	Description
	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> 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 issuing 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 issuing 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 under s 180w.
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:

Term (and section of the Act)	Description
	(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 (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 include: • 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 has 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.

Term (and section of the Act)	Description
Stored communications warrants issued in relation to a victim of a serious contravention s 116(1)(da)	Subject to other conditions being met, 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 we may make a suggestion 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 often the first line approach to 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 • the amount of data up / downloaded • the location of a mobile device from which a communication was made.
Telecommunications providers	Carriers and carriage service providers who supply certain carriage services over a telecommunications network, as defined in the Telecommunications Act 1997. Carriers in Australia include but are not limited to: • Telstra Corporation Ltd • Singtel Optus Pty Ltd • Vodafone Hutchison Australia Pty Ltd.

Term (and section of the Act)	Description
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 wrong 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 of lawfully accessed information under Chapter 3 of the Act complied with the prescribed requirements of the Act. 'Communication' is the communication of the information outside the agency, 'use' is the use of the information inside the agency, and 'recording' is the recording of the information, for example by creating copies.
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.