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 2020 to 30 June 2021
covering records from 1 July 2019 to 30 June 2020

Report by the acting 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 2020 to 30 June 2021
covering records from 1 July 2019 to 30 June 2020

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

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

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

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

Contents

Executive Summary

This report presents the results of inspections conducted by the Office of the Commonwealth Ombudsman (the Office) under s 186B of the *Telecommunications (Interception and Access) Act 1979* (the Act) from 1 July 2020 to 30 June 2021. These inspections examined agencies' records relating to stored communications and telecommunications data for the period 1 July 2019 to 30 June 2020. Where we did not inspect agencies during 2019–20, our 2020–21 inspections also covered records from earlier periods not previously inspected by our Office.

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

In 2020–21, we conducted inspections of 19[1] of the 20 agencies who have stored communications powers under Chapter 3 of the Act and 20 inspections of agencies' use of telecommunications data powers under Chapter 4 of the Act.

We made 29 recommendations in relation to 6 agencies. We also made 386 suggestions and 116 better practice suggestions across the agencies inspected.[2] A recommendation reflects a serious compliance issue or an issue on which an agency has not made sufficient progress in implementation. A suggestion reflects less serious and/or isolated issues where we consider an agency should take action to improve. Better practice suggestions highlight ways an agency might refine its practices where an existing practice may expose the agency to a risk of non-compliance.

Key issues we identified during 2020–21 inspections include:

- Stored communications: agencies not keeping records demonstrating that preservation notices were properly given; agencies applying for warrants relating to a victim of a serious contravention;[3] warrants issued by an ineligible authority; agencies' data vetting and quarantining processes; the destruction of stored communications.

[1] We did not inspect the Australian Securities and Investments Commission under Chapter 3 of the Act as the agency did not exercise these powers during the inspection period.

[2] For the previous 2019–20 inspection year, we made 21 recommendations in relation 3 agencies, 237 suggestions and 77 better practice suggestions.

[3] Serious contravention has the meaning given by s 5E of the Act, which in summary includes a serious offence or an offence punishable by at least 3 years imprisonment or by a fine of at least 180 penalty units (individual) or 900 penalty units (non-individual). Full definition is included in Appendix E - Glossary of terms.

- Telecommunications data: agencies not demonstrating that required considerations were taken into account by authorised officers; data vetting and quality assurance processes; Journalist Information Warrant (JIW) controls; use and disclosure of data received; meeting record-keeping obligations; and agency training and guidance material.

Generally, we saw an increase in the number of compliance-related findings compared to previous inspections. This partly reflects our increased emphasis on inspecting agencies' policies, procedures, and controls in place to mitigate risks of non-compliance. However, there were also instances where we were not satisfied with the remedial action agencies took in response to previous compliance findings, including implementing previous recommendations and suggestions made by our Office. In such instances, we made further recommendations or suggestions to agencies, including improving processes to prevent reoccurrence of issues we previously identified.

During our 2020–21 inspections, agencies proactively identified and disclosed several issues. Most agencies were receptive to our findings, demonstrating a commitment to either building or strengthening their culture of compliance.

Part A – Introduction

The Commonwealth Ombudsman has an overarching role in assessing agencies' compliance with Chapter 3 (preserving and accessing stored communications) and Chapter 4 (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. An agency must apply to an external issuing authority (such as a judge or eligible Administrative Appeals Tribunal member) for a warrant to access stored communications. Before a warrant is issued, an agency may authorise the 'preservation' of a stored communication to ensure it is retained by a carrier until the communication can be accessed under a warrant.

Telecommunications data is information about a communication but does not include the content or substance of that communication. Agencies may internally authorise access to this information, 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 for a Journalist Information Warrant (JIW) before it can make such an authorisation.

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 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, 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. However, where 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 an agency with a written report containing the results of our inspection and our assessment of its legislative compliance.

Each year the Ombudsman is required to report the results of our inspections to the Minister, 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 Minister.

This report is divided into 4 parts, with 3 appendices:

- **Part A** introduces our oversight of agencies' use of powers under Chapters 3 and 4 of the Act and the approach we took in the 2020–21 inspection period.
- **Part B** highlights the importance of agencies having a culture of compliance.
- **Parts C and D** set out the results of our stored communications and telecommunications data inspections.
- **Appendix A** sets out how we assess whether telecommunications data disclosed by the carrier, and used by the agency, complies with the authorisation given to access that data.
- **Appendix B** details our 2020–21 inspection schedule.
- **Appendices C** and **D** set out the criteria we used for our stored communications and telecommunications inspections.
- **Appendix E** provides a glossary of key terms used throughout the report.

As is the case in every reporting period, we made findings in relation to all agencies whose records we inspected during 2020–21. Our findings relate 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 at agencies. We emphasise that these examples are illustrative of findings or risks that are relevant to all agencies that exercise powers under Chapters 3 and 4 of the Act and not just the agencies about which the examples are written.

Agencies we oversee

During the 2019–20 record period[4], 20 agencies could use the stored communications and telecommunications data powers under the Act (see table in **Appendix B**). The Minister may declare additional agencies in prescribed circumstances but did not make any such declarations in 2019–20.

We do not have jurisdiction to oversee telecommunication service carriers, which hold the telecommunications data that agencies seek access to (for example, Telstra and Optus).

Inspections conducted in 2020-21

In 2020–21, our Office conducted 19 inspections of agencies' use of stored communications powers under Chapter 3 of the Act, and 20 inspections of agencies' use of telecommunications data powers under Chapter 4 of the Act.

The Act does not specify the frequency of inspections under Chapter 3 or 4 of the Act. Our Office scheduled inspections for all agencies which used the stored communications and telecommunications data powers during the record period 1 July 2019 to 30 June 2020.

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

There were 2 agencies whose records we could not inspect during the previous 2019–20 reporting period due to COVID-19 restrictions.[5] We inspected a sample of these agencies' records that were unable to be inspected in 2019–20 as part of our 2020–21 inspections.

Related investigation and inspections

Our oversight role under the Act is focused specifically on legislative compliance. However, our Office has broad jurisdiction under the *Ombudsman Act 1976* to investigate administrative actions and decisions of Australian Government agencies, either in response to a complaint or on the Ombudsman's 'own motion'. During the 2020–21 inspection period, in addition to inspections under the Act, our Office conducted an own motion investigation into the Australian Federal Police's (AFP) use and administration of telecommunications data powers from 2010 to 2020. The Ombudsman decided to conduct this investigation after the AFP disclosed that approximately 800 requests for access to location-based service data by ACT Policing was not previously reported to (and therefore not inspected

[4] Our inspections in 2020-21 considered use of the powers during 2019-20.

[5] Law Enforcement Conduct Commission's (LECC) compliance with Chapters 3 and 4 of the Act and Victoria Police's compliance with Chapter 3 of the Act.

by) our Office. We made 8 recommendations for improvement, including establishing the full extent of non-compliance and seeking legal advice regarding the implications of the unlawful accesses. Our report on the own motion investigation was published in April 2021 and is available on our website.[6] We continue to monitor the AFP's progress and will report on the AFP's implementation of these recommendations.

Sometimes we identify compliance issues with warrants or authorisations through our separate inspections of agencies' use of the industry assistance powers under Part 15 of the *Telecommunications Act 1997*. Part 15 provides for government and the communications industry to work together on law enforcement and national security investigations. Part 15 allows agencies to request or require technical assistance from providers. Agencies often use the industry assistance framework to support their use of other powers, including access to data under a telecommunications data authorisation. As a result, this report outlines some telecommunications data findings we identified through our industry assistance inspections under Part 15 of the *Telecommunications Act 1997.*

[6] *Australian Federal Police's (AFP) use and administration of telecommunications data powers 2010 to 2020 (ombudsman.gov.au).*

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 any remedial action they have already taken.

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

Stakeholder engagement

During 2020–21, 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 amendments 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 their 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 an accurate 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.

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

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

Another indicator of a strong culture of compliance is robust internal quality controls and quality assurance processes which enable agencies to proactively identify risks or issues that may lead to non-compliance with legislative requirements and take appropriate remedial and/or preventative action. Agencies should not rely on our Office to identify instances of non-compliance or provide solutions for issues identified. It is important that agencies proactively and contemporaneously assess their own records and take appropriate remedial action.

Our Office encourages agencies to seek our review and feedback when developing new processes, templates, and guidance materials, or where advice is needed to address an emerging issue. This may be during inspections or during the period between inspections.

Agencies with a strong culture of compliance also demonstrate transparency in disclosing issues to the Office and respond positively to our feedback, recognising it as an opportunity for improvement. These agencies are also better able to adapt their training and internal guidance in response to changes in legislation, policy, and procedures.

In 2020–21 we were pleased to observe several good practices among agencies, notably the establishment or continuation of centralised compliance functions (for example at WA Police). 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. [7]

We will continue to work with all agencies to support a strong culture of compliance.

[7] Stored communications – Australian Criminal Intelligence Commission, Crime and Corruption Commission (Queensland), New South Wales Crime Commission, New South Wales Police Force, Queensland Police Service and Western Australia Police.
Telecommunications Data – Australian Competition and Consumer Commission, Australian Securities and Investments Commission and Corruption and Crime Commission (Western Australia).

Part C – Stored communications

Stored communications and the Commonwealth Ombudsman's oversight function

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

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

To access stored communications, an agency must apply to an external issuing authority (such as a Judge or eligible Administrative Appeals Tribunal (AAT) member) for a stored communications warrant. A stored communications warrant authorises an agency to access stored communications held by a carrier that were made or intended to be received by the person in respect of whom the warrant was issued, subject to any conditions or restrictions 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.[8]

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 accurate information to make the required considerations when deciding whether to issue a stored communications warrant.

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

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 2020–21 is set out at **Appendix C**.

Summary of stored communications findings

During 2020–21, our Office inspected 19 agencies' access to stored communications under Chapter 3 of the Act.[9] For most agencies our inspections covered records for the period 1 July 2019 to 30 June 2020.[10] For our stored communications inspections conducted during 2020–21 we made:

- 6 recommendations across 3 agencies
- 124 suggestions, and
- 49 better practice suggestions.

This was an increase from the 2019–20 figures of 2 recommendations made to one agency, 73 suggestions and 29 better practice suggestions, reflecting an overall increase in the number of findings and some repeated findings from the previous period.

Most 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 other instances where we were not satisfied with the remedial action taken by agencies. In such instances, we made further suggestions or recommendations including improving processes to prevent reoccurrence of the issue.

[9] We did not inspect the Australian Securities and Investments Commission (ASIC) as they did not use the powers under Chapter 3 of the Act during the period.

[10] Due to the impacts of COVID-19 on our 2019–20 inspection schedule, for the LECC our inspection covered records for the period 1 July 2017 to 30 June 2020. For Victoria Police, our inspection covered records for the period 1 July 2018 to 30 June 2020.

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 2020–21

The table below sets out the number of recommendations, suggestions and better practice suggestions made by our Office to each agency during this period. It is important to note that a higher aggregate number of findings does not translate to poorer compliance on behalf of an agency, as findings vary in their significance. The impact of non-compliance varies depending on the nature of the finding.

Table 1 – Number of recommendations, suggestions, and better practice suggestions made per agency during the 2020–21 inspection period (figures from the 2019-20 inspection period are included in brackets)

Agency	Recommendations	Suggestions	Better practice suggestions
Australian Competition and Consumer Commission (ACCC)	- (-)	8 (4)	3 (2)
Australian Criminal Intelligence Commission (ACIC)	- (-)	4 (1)	2 (2)
Australian Commission for Law Enforcement Integrity (ACLEI)	- (-)	6 (1)	1 (1)
Australian Federal Police (AFP)	2 (-)	22 (12)	6 (4)
Crime and Corruption Commission (Queensland) (CCC QLD)	- (-)	1 (7)	2 (2)
Corruption and Crime Commission (Western Australia) (CCC WA)	- (-)	- (-)	- (-)
The Department of Home Affairs (the Department)	- (-)	4 (5)	5 (2)
Independent Broad-based Anti-corruption Commission (IBAC)	- (-)	4 (1)	2 (1)

Agency	Recommendations	Suggestions	Better practice suggestions
Independent Commission Against Corruption New South Wales (ICAC NSW)	- (-)	10 (8)	2 (1)
Independent Commissioner Against Corruption (South Australia) (ICAC SA)	- (-)	- (3)	- (1)
Law Enforcement Conduct Commission (LECC)	- (not inspected in 2019-20)	12	4
New South Wales Crime Commission (NSW CC)	- (-)	1 (-)	2 (2)
New South Wales Police Force (NSW PF)	- (-)	4 (8)	2 (3)
Northern Territory Police (NT Police)	- (-)	5 (6)	2 (-)
Queensland Police Service (QPS)	- (-)	2 (3)	1 (3)
South Australia Police (SA Police)	- (-)	10 (1)	1 (3)
Tasmania Police	1 (2)	12 (9)	8 (1)
Victoria Police	3 (not inspected in 2019-20)	10	4
Western Australia Police (WA Police)	- (-)	9 (1)	2 (1)
TOTAL:	**6 (2)**	**124 (73)**	**49 (29)**

Table 1 – Use of stored communications powers and records inspected in the 2020-21 period

Agency	Records period inspected	Total Historic PN[11]	Historic Inspected	Total Ongoing PN[12]	Ongoing inspected	Stored Comms Warrants	Warrants inspected	Destructions	Destructions inspected
ACCC	19-20	27	**21**	-	**-**	12	**12**	8	**8**
ACIC	19-20	2	**2**	7	**7**	2	**2**	-	**-**
ACLEI	19-20	1	**1**	1	**1**	2	**2**	-	**-**
AFP[13]	19-20	144	**21**	79	**12**	79	**38**	31	**22**
CCC QLD	19-20	3	**0[14]**	26	**16**	6	**6**	15	**15**
CCC WA	19-20	-	**-**	3	**3**	1	**1**	-	**-**
The Department	19-20	15	**15**	-	**-**	2	**2**	-	**-**
IBAC	19-20	1	**1**	5	**5**	1	**1**	-	**-**
ICAC NSW	19-20	1	**1**	1	**1**	2	**2**	-	**-**
ICAC SA	19-20	-	**-**	1	**1**	-	**-**	-	**-**
LECC	17-18 18-19 19-20	2	**2**	24	**24**	11	**11**	-	**-**
NSW CC	19-20	-	**-**	4	**4**	3	**3**	2	**2**
NSW PF	19-20	794	**31**	132	**5**	831	**36**	48	**7**
NT Police	19-20	6	**6**	25	**25**	2	**2**	-	**-**
QPS	19-20	61	**12**	269	**43**	181	**47**	237	**49**
SA Police	19-20	91	**14**	29	**6**	34	**19**	2	**2**
Tasmania Police	19-20	25	**6**	82	**15**	37	**21**	53	**22**
Victoria Police	18-19 19-20	126	**32**	160	**34**	233	**61**	139	**17**
WA Police	19-20	59	**9**	71	**20**	104	**39**	20	**20**

[11] Preservation Notices (PN). This is the total of preservation notices reported to our Office. In some instances, we made findings where the number of preservation notices reported to our Office did not reflect the actual number of preservation notices given by the agency.

[12] This is the total of preservation notices reported to our Office. In some instances, we made findings where the number of preservation notices reported to our Office did not reflect the actual number of preservation notices given by the agency.

[13] We also inspected all 8 foreign preservation notices given by the AFP.

[14] We did not inspect any historic preservation notices as we focused on the preservation notices that led to stored communications accessed under a stored communications warrant.

Compliance issues and risks to compliance

This section outlines instances of non-compliance identified across multiple agencies during the 2020–21 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 2020–21 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:

- warrants issued by an ineligible authority
- agencies applying for stored communications warrants in relation to a victim of a serious contravention
- agencies not demonstrating that preservation notices were properly given and maintaining records
- agencies' data vetting and quarantining processes
- agencies' destruction of stored communications, and
- agencies using, communicating, and recording stored communications.

Warrants issued by an ineligible authority

Under s 110(1) of the Act, a criminal law-enforcement agency may apply to an 'issuing authority' for a stored communications warrant in respect of a person.

The term 'issuing authority' is defined under s 5(1) of the Act as "a person in respect of whom an appointment is in force under section 6DB". Under s 6DB(1) of the Act, the Attorney-General may appoint the following, in writing, to be an issuing authority:

- a Judge
- a Magistrate, and
- certain AAT members.

Where an AAT member, Judge or Magistrate is not an 'issuing authority' within the meaning of the Act, any warrants issued by the person are invalid and can impact the use, communication or recording stored communications received by agencies under the warrant.

We made 1 recommendation and 3 suggestions across 2 agencies[15] during our 2020–21 inspections about ensuring warrant applications are presented to eligible issuing authorities and taking appropriate action where stored communications information be accessed under a warrant not issued by a person who is not an 'issuing authority'.

Warrants issued by ineligible AAT member

Following our previous inspection, Victoria Police disclosed instances where stored communications warrants were issued by a member of the AAT who was not

[15] The Victoria Police and the Tasmania Police.

appointed under s 6DB(1) of the Act. We suggested that Victoria Police quarantine all stored communications obtained under these warrants and seek advice regarding the legality of the warrants and any use or communication of the accessed information.

We reviewed action taken during our 2020–21 inspection, including a register maintained by Victoria Police to track the status of warrants affected by this issue. We identified instances where the stored communications accessed under the invalid warrants were not quarantined and appeared to have been used or communicated. Our Office raised concerns regarding the accuracy and adequacy of Victoria Police's register, the management of this information and the absence of record-keeping.

We recommended that Victoria Police immediately quarantine and cease any further use and communication of stored communications information accessed under affected warrants until it completed the actions listed in our earlier recommendations, including that Victoria Police:

- review the accuracy of its record-keeping for the affected warrants and investigations, including confirming the exact number of affected warrants, the extent of any use and communication of information accessed under affected warrants, and the relevant details of any disclosures
- obtain written advice on each instance of use and communication, and what remedial action should be taken.

In response, Victoria Police advised that all affected stored communications were quarantined. Victoria Police also referred to further written advice and other records relevant to their management of this issue that were not available to our Office at the time of our 2020–21 inspection. Victoria Police advised this further information will be available to our Office for our 2021–22 inspection.[16]

Warrants issued by ineligible Magistrate

Following our 2020–21 inspection at Tasmania Police, we identified 2 instances where stored communications warrants were issued by a Magistrate who did not have an appointment in force under s 6DB(1) of the Act. We previously raised a similar issue with Tasmania Police in our 2018 inspection (where 2 Magistrates issued 4 warrants but were not eligible issuing authorities).

[16] Following our 2020–21 inspection, we engaged further with Victoria Police in relation to this issue. Victoria Police has provided information demonstrating that it has now taken appropriate action in response to our recommendations. Our Office will continue to monitor for any future occurrences of this issue during our inspections across all agencies.

Tasmania Police advised our Office that, at the time the 2 identified warrants were applied for, enquiries were made regarding the eligibility of the Magistrate and that Tasmania Police was satisfied the Magistrate was authorised based on a copy of an application to be appointed as an issuing authority. It appears that despite this application, the Magistrate was not in fact appointed.

We advised Tasmania Police that it should quarantine all stored communications obtained and seek legal advice regarding any use or communication of the accessed information. Tasmania Police subsequently identified an additional instance occurring in the 2020–21 records period.

Tasmania Police advised our Office it quarantined the stored communications for all 3 identified affected records, has commenced enquiries with investigators regarding any use and communication and would obtain legal advice regarding these matters.

We recommended that Tasmania Police should ensure that, prior to applying for a warrant, it confirms the person is appointed under s 6DB(1) of the Act to issue stored communications warrants.

In response, Tasmania Police advised that they had quarantined all affected data and taken action to manage any use or communication in accordance with advice received. Tasmania Police also informed our Office that it maintains a current list of issuing authorities and ensures warrant applications are presented to eligible issuing authorities.

Stored communications warrants 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 expensive. If a victim has an opportunity to consent and they do not wish their stored communications to be accessed, then an agency must not use s 116 of the Act to access their stored communications. If a victim declines to give their consent, their reasons for doing so are immaterial.

Where agencies pursue a stored communications warrant in relation to a victim of a serious contravention, they should ensure 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 2 suggestions across 2 agencies[17] during our 2020–21 inspections about addressing the special considerations regarding access to victims' stored communications and maintaining records

Policies and procedures should address special considerations regarding access to victims' stored communications

Victoria Police's policy and procedural documents in relation to accessing stored communications did not directly address the special considerations required given the unique status afforded to victims by virtue of s 116(1)(da) of the Act. Namely, that an issuing authority may only issue a stored communications warrant if satisfied the victim is 'unable' to consent, or it is 'impracticable' for the person to consent to their communications being accessed.

We suggested Victoria Police update its policy, procedures and templates to ensure the special considerations for issuing a stored communications warrant in relation to a victim under s 116(1)(da) of the Act are clearly outlined. In addition, where any ambiguity arises in relation to a victim's ability to give consent at the time of a stored communications warrant application, we suggested Victoria Police seek (and retain on record) specific advice. Victoria Police advised it actioned these suggestions.

Warrant applications should demonstrate special considerations regarding access to victims' stored communications

We identified 2 instances where the AFP's applications for stored communications warrants did not clearly demonstrate full consideration of s 116(1)(da) of the Act regarding the victim's inability to consent or it being impracticable for the victim to consent. The guidance and affidavit templates used did not refer to s 116(1)(da) of

[17] The AFP and the Victoria Police.

the Act. We considered this could impact the issuing authorities' ability to make fully informed decisions.

We suggested the AFP ensure affidavits accurately reflect whether consent was sought where a stored communications warrant is sought in relation to a victim of a serious contravention. Where consent was not sought, the AFP should clearly demonstrate how the thresholds of 'unable' or 'impracticable' were met. In response, the AFP noted its view that sufficient information was provided to the issuing authorities in the 2 instances identified, however advised it would update guidance and templates in line with our suggestion.

Demonstrating that preservation notices were properly given and maintaining records

A person giving a domestic preservation notice must be satisfied the conditions for giving domestic preservation notices under s 107J(1) of the Act are met. Agencies are required under the Act to keep records of each preservation notice given, and documents or other materials indicating whether the notice was properly given (under s 151(1)(a) of the Act). We do not consider template wording alone is sufficient to demonstrate that preservation notices are properly given in accordance with the conditions under s 107J(1) of the Act, nor to meet the record-keeping obligations under s 151(1)(a) of the Act, as the circumstances behind each preservation notice given will necessarily differ.

Agencies should have a consistent process to capture information indicating whether a preservation was properly given. This process should capture information relevant to the decision to give a preservation notice and the conditions for giving a preservation notice, such as the information linking the subject of the notice (such as the service number or person) to the relevant investigation and how the stored communications might assist in connection with the investigation. While persons giving preservation notices may have an existing understanding of the relevant facts of an investigation, agencies must be able to demonstrate this through records. Along with the requirement to keep records under the Act, in the absence of an established, consistent process, our Office may not be satisfied that preservation notices are given in compliance with the legislation.

We made 17 suggestions across 12 agencies[18] during our 2020–21 inspections about demonstrating that preservation notices were properly given and maintaining records. Our suggestions included:

[18] The NSW ICAC, the NT Police, the IBAC, LECC, the QPS, ACLEI, the AFP, the Department, the WA Police, the NSW Police, the Victoria Police and the Tasmania Police.

- ensuring records contain sufficient information to demonstrate that the person giving the preservation notice turned their mind to all relevant conditions under s 107J(1) of the Act
- implementing a consistent process to capture information that indicates whether a preservation notice was properly given
- ensuring records demonstrate that any amendments to preservation notice request forms are made before the preservation notice is given and demonstrate the updated information is available for consideration by the person who is giving the preservation notice in making their decision, and
- ensuring that records are kept capturing information that indicates whether preservation notices were properly given, as required by s 151(1)(a) of the Act.

Processes to keep records to demonstrate preservation notices are properly given

We identified the QPS did not have an established process for keeping records indicating whether a preservation notice was properly given. We were not satisfied the QPS was consistently meeting its record-keeping obligations under s 151(1)(a) of the Act. This is the second consecutive report where our Office made this finding.

We suggested the QPS implement a consistent process to ensure it meets 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, QPS advised it engaged with another state-based law enforcement agency to assist with establishing a 'best practice' solution to enhance its record-keeping practices and will obtain guidance and feedback from our Office as processes are developed.

Use of template wording in preservation notices

Preservation notices given by ACLEI contained template wording setting out the legislative requirements of s 107J(1)(c) of the Act but did not contain information linking the telecommunications service or person specified in the preservation notice to the offence being investigated.

We suggested ACLEI implement a consistent process to ensure it meets its obligations under s 151(1)(a) of the Act to keep records indicating whether a preservation notice was properly given. In response, ACLEI advised it was developing a template to document this information and updated Standard Operating Procedures.

Use of stamps instead of signatures on preservation and revocation notices

We identified a practice where revocation notices for preservation notices were 'signed' by WA Police warrant administration staff using signature stamps aligning with the signatures of authorised officers. This process occurred without involvement from the authorised officer. In addition, although we were satisfied that preservation notice *requests* were physically signed by the authorised officer, the actual preservation *notices* were not signed by the authorised officer but instead 'signed' by the WA Police warrant administration staff using the signature stamp. As there were no time stamps, we could not conclusively determine that the preservation notices were only sign-stamped on behalf of the authorised officer after the authorised officer made the decision to give the preservation notice. This created ambiguity in the records as to whether the preservation notices were properly given.

We suggested the WA Police cease the practice of warrant administration staff using signature stamps on behalf of authorised officers for revocations and amend revocation processes to be compliant with the Act. We also suggested the WA Police seek advice regarding the practice of signing preservation notices on behalf of authorised officers. In response, WA Police advised it amended relevant process documents accordingly and ceased this practice.

Data vetting and quarantining processes

Any stored communications received outside the parameters of the relevant stored communications warrant are unauthorised and should be quarantined from use or communication. It is important that an agency has processes to vet data received, identify any unauthorised stored communications received outside the parameters of the warrant and effectively quarantine any such content.

In assessing agencies' data vetting and quarantining processes, our Office looks for records demonstrating action taken to quarantine any unauthorised stored communications received outside the parameters of the warrant and confirmation that the information was not used, communicated, or recorded. In the absence of established agency procedures, there is a risk that data vetting may not occur consistently and, therefore, unauthorised content may not be identified and quarantined from use or communication.

When agencies identify non-compliant stored communications were received, these should be quarantined to ensure the information is not used or communicated. Effective and immediate remedial action mitigates ongoing risks that may eventuate from the non-compliance, for example that unlawfully obtained evidence may be used for prosecutorial purposes or, the privacy of individuals may be breached through receipt of data outside the parameters of a warrant or authorisation. We encourage

agencies to seek advice on the nature of the non-compliance and whether further use or communication of the stored communications under the Act is permissible.

We made 1 recommendation, 21 suggestions and 3 better practice suggestions regarding data vetting and quarantining policies and procedures across 8 agencies[19] during our 2020–21 inspections. Our suggestions included establishing policies and procedures for data vetting and quarantining, as well as implementing additional controls where to strengthen or address gaps in existing practices.

Data vetting policies and procedures

As a result of our 2019–20 inspection, we suggested the ICAC NSW incorporate guidance into its policy and procedural documents to ensure data vetting is conducted consistently and establish a consistent mechanism for quarantining stored communications product not within the parameters of a warrant.

While the ICAC NSW updated its data vetting and quarantining procedures, during our 2020–21 inspection there remained some instances in a specific system used by ICAC NSW where we were unable to be satisfied that the stored communications were within the parameters of the warrant. We also noted the ICAC NSW's data vetting procedures did not include instructions for confirming that the relevant carrier accessed the stored communications while the relevant warrant was in force.

We suggested the ICAC NSW develop data vetting processes for vetting stored communications in its system to ensure it can accurately confirm all stored communications were provided in accordance with the parameters of the warrant and quarantine any stored communications where it is unable to make this determination. We also suggested the ICAC NSW introduce an additional assessment into its data vetting procedures to ensure it can identify and appropriately manage any instances where stored communications are accessed by the carrier after the warrant ceased. ICAC NSW advised it developed a process for vetting communication in its system to ensure it can determine compliance.

In practice the ACCC vets stored communications received against the parameters of the warrant. We did not identify any instances of the ACCC receiving stored communications outside the parameters of the warrant. However, we identified the ACCC does not have established policy guiding its data vetting processes, exposing the ACCC to a risk of non-compliance.

We suggested the ACCC establish data vetting procedures in our previous inspection report. In this report, we again suggested the ACCC finalise its policy and procedures on data vetting as a priority to ensure this is done consistently. We also suggested the ACCC finalise a consistent method for quarantining unauthorised accessed data

[19] The ACCC, ACLEI, the AFP, the ICAC NSW, Tasmania Police, SA Police, the IBAC and the Department.

as a priority to limit the risk of dealing with this information. In response, the ACCC advised that processes were being revised to ensure a consistent approach to data vetting and quarantining.

Destruction of stored communications

Where the chief officer of an agency is satisfied that information or a record obtained by accessing a stored communication is not 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 stored communications information.

Achieving compliance with destruction requirements requires agencies to have a strong framework in place to track all relevant stored communications, seek appropriate approval for destruction from the chief officer or their delegate, and 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.

We made 20 suggestions and 14 better practice suggestions regarding destruction of stored communications across 14 agencies[20] during our 2020–21 inspections. Our suggestions included:

- establishing a destruction regime enabling agencies to identify, on a periodic basis, whether stored communications information or records are likely to be required for a purpose referred to in s 150(1)(b) of the Act
- establishing an internal agency timeframe for destroying records 'forthwith'
- ensuring agencies destroy both originals and copies of stored communications in accordance with s 150(1) of the Act
- agencies review destruction processes and implement a process to help locate all stored communications records in agencies' possession to ensure all stored communications records are destroyed forthwith in accordance with s 150(1) of the Act, and
- agencies keep records to meet their obligations under s 151(1)(i) of the Act. [21]

Establishing a destruction regime that includes periodic review of stored communications records

SA Police made several disclosures during our 2020–21 inspection including copies of stored communications information being inadvertently destroyed without authorisation, significant delay in seeking authorisation to destroy when stored communications were no longer required, and there may be some stored communications information or records no longer required that were not destroyed. In this last instance, the delay was due to SA Police seeking advice on appropriate delegations under s 150(1) of the Act.

We suggested SA Police establish a destruction regime enabling it to identify, on a periodic basis, whether stored communications information or records are likely to be required for a purpose referred to in s 150(1) of the Act. The destruction regime should include appropriate training and guidance materials to ensure compliance.

We also suggested SA Police review existing stored communications information and records to determine if these are no longer required and, with appropriate authorisation in place, destroy any such stored communications information or records as soon as possible in accordance with s 150(1) of the Act. We also made a better practice suggestion that SA Police establish an internal timeframe for destroying records 'forthwith.'

[20] The SA Police, the ACIC, LECC, the NT Police, the NSW Police, the Department, the NSW CC, the WA Police, ACLEI, the NSW ICAC, the QPS, IBAC, Victoria Police and Tasmania Police.
[21] Section 151(1)(i) establishes an obligation to ensure the agency keeps a record of documents indicating whether information or a record was destroyed in accordance with s 150 of the Act.

In response, SA Police advised that a review was conducted and, once the appropriate delegations were acquired, records identified as no longer being required will be destroyed. SA Police advised that a standard operating procedure is being developed.

Destructions not completed 'forthwith'

In both the 2019–20 and 2020–21 inspections, we identified that WA Police had no internal defined timeframes for destructions, and we identified instances where WA Police did not complete stored communications destructions 'forthwith'. For example, some stored communications were still accessible during our inspection, 10 months after being certified for destruction. We also identified further instances where stored communications information was still accessible after being certified for destruction. In addition, we found the WA Police's standard operating procedure referred to ensuring that a Commonwealth Ombudsman inspection occurred regarding the relevant record period before destruction under s 150(1) of the Act takes place. We do not consider retaining information or records obtained under a stored communication warrant for the purpose of our inspections to be a 'permitted purpose' under the Act.

We suggested WA Police review destructions undertaken to date and take action to ensure stored communications are destroyed in accordance with the relevant destruction authorisation. We also suggested WA Police ensure all stored communications records are destroyed forthwith in accordance with s 150(1) of the Act and it reviews its destruction process and implement a process to assist its ability to locate all stored communications records in its possession.

We also made better practice suggestions that the WA Police update their destructions policies and guidance material to reflect current practices and accurately reflect the legislative requirements as well as include a definition of 'forthwith'. In response, the WA Police advised it has implemented measures to track copies of stored communications and updated standard operating procedures.

Using, communicating, and recording stored communications

In assessing compliance with s 151(1)(h) of the Act, we consider whether an agency has effective processes to meet its record-keeping obligations regarding using, communicating, and recording stored communications under Chapter 3 of the Act. It is important that agencies have a consistent process for documenting these actions to:

- accurately account for whether stored communications were used, communicated, or recorded for a permitted purpose under Chapter 3 of the Act
- demonstrate that any unauthorised stored communications information obtained outside of the parameters of a warrant has been quarantined and managed appropriately

- track copies of stored communications and records to fulfil destruction requirements, and
- ensure they can satisfy record-keeping obligations under s 151(1)(h) of the Act.

We made 8 suggestions and 3 better practice suggestions regarding use, communications and recording of stored communications across 10 agencies[22] during our 2020–21 inspections.

During our inspections we observed 2 distinct issues. The first was where agencies did not have established procedures in place to meet their record-keeping obligations regarding using, communicating, and recording stored communications. The second related to agencies which had established procedures but where these did not enable the agency to effectively demonstrate it meets record-keeping obligations.

We made suggestions that these agencies establish a consistent process for keeping records to accurately account for whether stored communications were used, communicated, or recorded for a permitted purpose and ensuring agencies satisfy their record-keeping obligations under s 151(1)(h) of the Act. These suggestions included developing and implementing measures such as centralised databases or registers, clear procedural guidance to staff and/or formalised procedural documentation and instructions.

Centralised registers for use and communication of stored communications information

The IBAC's procedures instructed staff to use a centralised log to record use and communication of stored communications information, however we observed inconsistent decentralised processes across different teams.

We acknowledge the IBAC's processes relating to communicating, using or recording stored communications information were under review by the IBAC at the time of our inspection.

We made a better practice suggestion that the IBAC re-establish and maintain a centralised register for use and communication of stored communications information. In response, the IBAC advised it would amend its stored communications register template to ensure all use and communication is included in the register for the relevant operation.

The ACIC does not maintain a centralised database for communicating, using or recording lawfully accessed information, and ACIC guidance material does not address record-keeping requirements under s 151(1)(h) of the Act.

[22] The IBAC, the ACIC, the WA Police, ACLEI, the ACCC, the AFP, the Department, the NSW ICAC, LECC, and Victoria Police.

We suggested the ACIC provide clear guidance to staff for recording use, communication and recording of stored communications to accurately account for whether stored communications were used, communicated, or recorded for a permitted purpose, and ensure it can satisfy its record-keeping obligations under s 151(1)(h) of the Act. The ACIC subsequently implemented a Warrant Information Minute Log to record the use, communication and recording of stored communication information.

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.

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

Telecommunications data includes, but is not limited to:

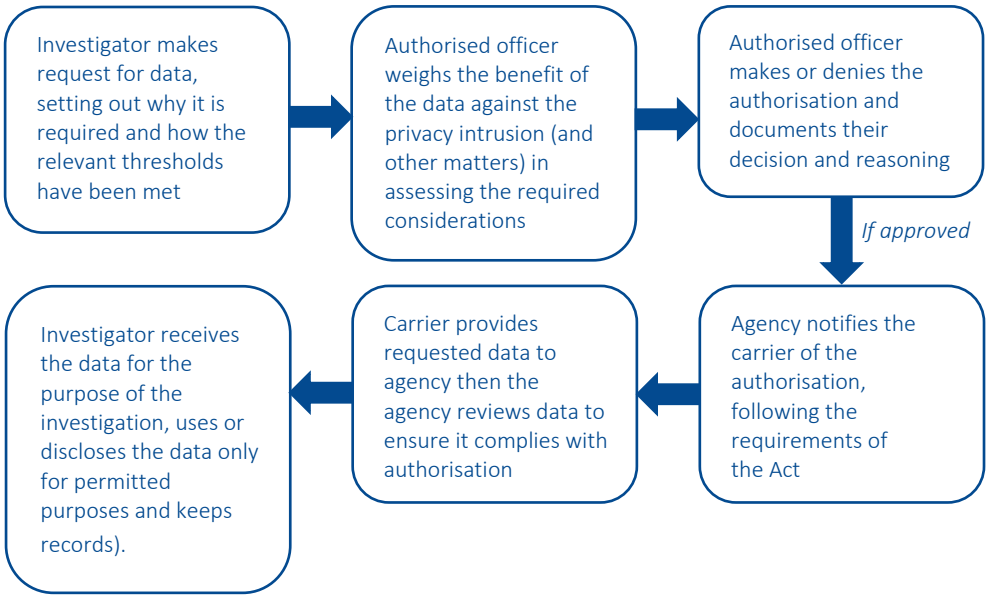
- subscriber information (for example the name, date of birth and address of the person to whom a service is subscribed)
- date, time, and duration of a communication
- phone number or email address of the sender and recipient of a communication
- Internet Protocol (IP) address used for a session
- start 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).

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.

Our Office does not review the merits of a 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. Unlike Chapters 2 and 3 of the Act (interception and stored communications), the decision to authorise the covert intrusion into somebody's privacy under Chapter 4 (telecommunications data) is made by the agency investigating, not an external issuing authority.

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

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[23]. We look at the background material in the request documents to be satisfied that authorised officers had enough information to assess the required considerations.

We also assess the processes agencies have in place to request telecommunications data, make authorisations, notify the carriers, and manage the data once it is received. We check agencies maintain records demonstrating that any disclosure or use of telecommunications data complied with the requirements of the Act. We assess agencies' compliance with the Act by looking at individual files in detail alongside holding discussions with key agency staff involved in the processes and reviewing supporting procedures, guidance, training, and the general approach of agencies to using these powers.

[23] See Appendix E - Glossary of terms.

Summary of telecommunications data findings

During 2020–21, our Office inspected 20 agencies' access to telecommunications data under Chapter 4 of the Act. Our inspections covered records for the period 1 July 2019 to 30 June 2020.[24] For our telecommunications data inspections conducted during 2020–21 we made:

- 23 recommendations across 6 agencies
- 273 suggestions, and
- 67 better practice suggestions.

This was an increase from the 2019–20 figures of 15 recommendations made across 3 agencies, 165 suggestions and 48 better practice suggestions and reflects an increase in the number of findings and repeat issues identified at many agencies in the period.

While some agencies demonstrated high levels of compliance with the Act, others had significant issues leading to multiple recommendations and suggestions from our Office. Agencies we inspect are diverse in size and operating environment, and this is reflected in the volume and type of requests for access to telecommunications data.

Maintaining a sufficient level of awareness of the Act's requirements among relevant staff is an ongoing challenge for agencies. We generally identified lower levels of staff compliance awareness in agencies that do not provide regular and tailored compliance training compared to agencies conducting regular structured training with relevant staff. Typically, at larger agencies, there are higher numbers of requesting and authorised officers (who may be geographically dispersed) and regular staff changes. While it can be more challenging to deliver in larger geographically dispersed agencies, regular targeted training, and comprehensive guidance documentation for supporting officers is critical to achieve compliance with the Act. Consequently, where we did identify compliance issues, we commonly made recommendations and suggestions to agencies about implementing effective training and providing sufficient guidance documentation to support officers.

Recommendations and suggestions made during 2020–21

The table below sets out the number of recommendations, suggestions and better practice suggestions made by our Office to each agency during this period. It is important to note that a higher aggregate number of findings does not translate to poorer compliance on behalf of an agency, as findings vary in their significance. The impact of non-compliance varies depending on the nature of the finding.

[24] In one instance where an agency had not been inspected in the 2 previous inspection periods, we assessed records from earlier periods during our 2020-21 inspection. In another instance, we were unable to finalise our inspection of an agency during the 2019-20 financial year due to COVID-19 impacts. That inspection considered records from the 2017-18 and 2018-19 periods and was finalised in November 2020, the results of which are included in this report, along with the results of that agency's 2020-21 inspection.

Table 4 – Number of recommendations, suggestions, and better practice suggestions made per agency during the 2020–21 inspection period (figures from the 2019-20 inspection period are included in brackets)

Agency	Recommendations	Suggestions	Better practice suggestions
Australian Competition and Consumer Commission (ACCC)	- (-)	3 (5)	1 (3)
Australian Criminal Intelligence Commission (ACIC)	- (-)	8 (5)	4 (1)
Australian Commission for Law Enforcement Integrity (ACLEI)	- (-)	16 (7)	3 (3)
Australian Federal Police (AFP)	4 (-)	16 (13)	4 (3)
Australian Securities and Investments Commission (ASIC)	- (-)	10 (4)	7 (4)
Crime and Corruption Commission (Queensland) (CCC QLD)	- (-)	8 (4)	3 (3)
- JIW review	-	4	1
Corruption and Crime Commission (Western Australia) (CCC WA)	- (-)	5 (3)	1 (3)
The Department of Home Affairs (the Department)	- (3)	12 (20)	7 (3)
Independent Broad-based Anti-corruption Commission (IBAC) (2019-20)[25]	-	15	3
Independent Broad-based Anti-corruption Commission (IBAC) (2020-21)	-	15	2
Independent Commission Against Corruption New South Wales (ICAC NSW)	- (-)	9 (9)	- (1)

[25] Our 2019-20 inspection of IBAC for the periods 1 July 2017 to 30 June 2018 and 1 July 2018 to 30 June 2019 commenced in March 2020 but was paused due to the COVID-19 pandemic, the remainder of the inspection was conducted in November 2020.

Agency	Recommendations	Suggestions	Better practice suggestions
Independent Commissioner Against Corruption (South Australia) (ICAC SA)	- (-)	7 (10)	1 (8)
Law Enforcement Conduct Commission (LECC)	- (not inspected in 2019-20)	11[26]	3
New South Wales Crime Commission (NSW CC)	- (-)	9 (4)	3 (-)
New South Wales Police Force (NSW PF)	- (9)	19 (12)	1 (2)
Northern Territory Police (NT Police)	3 (-)	16 (16)	7 (-)
Queensland Police Service (QPS)	2 (-)	11 (12)	- (8)
South Australia Police (SA Police)	5 (-)	26 (12)	3 (3)
Tasmania Police	6 (3)	10 (13)	5 (-)
- JIW review	-	4	-
Victoria Police	3 (-)	22 (10)	4 (2)
Western Australia Police (WA Police)	- (-)	17 (5)	4 (1)
TOTAL:	**23 (15)**	**273 (164)**	**67 (48)**

[26] Correspondence was received from the LECC formally disagreeing with several findings made during the inspection. The 2021–22 inspection conducted by our Office amended several findings made during the 2020–21 inspection. Figures provided in this table reflect the amended figures.

Table 5 – Use of telecommunications data powers and records inspected in the 2020–21 period

Agency	Records period inspected	Total Historic[27]	Historic Inspected	Total Prospective[28]	Prospective inspected
ACCC	19-20	109	**20**	-	**-**
ACIC	19-20	5,298	**61**	1,116	**59**
ACLEI	19-20	264	**50**	34	**23**
AFP	19-20	18,975	**93**	6,301	**28**
ASIC	19-20	1,474	**37**	25	**12**
CCC QLD	19-20	712[29]	**31**	151	**30**
CCC WA	19-20	207	**48**	94	**38**
Department of Home Affairs	19-20	3,192	**32**	295	**23**
IBAC	17-18	717	**11**	311	**16**
	18-19	550	**26**	333	**23**
	19-20	497	**55**	284	**51**
ICAC NSW	19-20	175	**20**	31	**12**
ICAC SA	19-20	195	**32**	19	**10**
LECC	17-18	414	**20**	50	**10**
	18-19	765	**23**	98	**11**
	19-20	484	**55**	40	**24**
NSW CC	19-20	4,737	**61**	1,716	**60**
NSW PF	19-20	119,472	**82**	1,395	**14**

[27] In some instances, we made findings where the number of authorisations reported to our Office did not reflect the actual number of authorisations made by the agency.
[28] In some instances, we made findings where the number of preservation notices reported to our Office did not reflect the actual number of preservation notices given by the agency.
[29] This figure includes one authorisation under a Journalist Information Warrant (JIW).

Agency	Records period inspected	Total Historic[27]	Historic Inspected	Total Prospective[28]	Prospective inspected
NT Police [30]	19-20	Unable to be determined	**72**	Unable to be determined	**27**
QPS	19-20	25,455	**60**	4,199	**33**
SA Police	19-20	7,221	**34**	466	**28**
Tasmania Police	19-20	3,892	**39**	115	**39**
Victoria Police	19-20	102,908	**45**	14,827	**35**
WA Police	19-20	26,757	**63**	3,024	**61**

Journalist Information Warrants (JIWs)

Agency	Records period inspected	JIWs	JIW authorisations	JIW authorisations inspected
CCC QLD	19-20	1	1	1

Authorisations issued for telecommunications data on behalf of foreign countries

Agency	Foreign Historic	Foreign Historic Inspected	Foreign Prospective	Foreign Prospective Inspected
AFP	66	**30**	-	**-**

[30] During the inspection the exact number of occasions when NT Police exercised its use of telecommunications data powers could not be accurately reconciled. This issue was highlighted as part of the findings for the NT Police 2020-21 formal report.

Compliance issues and risks to compliance

This section outlines instances of non-compliance identified across multiple agencies during 2020–21 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 2020–21 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:

- demonstrating authorised officer considerations
- data vetting and quality control frameworks
- Journalist Information Warrant controls
- use and disclosure of record-keeping obligations, and
- availability and quality of training and guidance material.

Related findings from Industry Assistance (IA) inspections

Our Office inspects IA records to determine agencies' compliance with Part 15 of the *Telecommunications Act 1997.*[31] We assess both the IA records and any related authorisations and warrants from other regimes subject to our oversight including telecommunications data.

The IA regime relies on existing legislative safeguards and protections governing how agencies request and receive personal information from designated communications providers (DCPs). Therefore, it is important that warrants and authorisations used in conjunction with IA powers are properly applied for and authorised.

In 2 of the 3 agencies whose use of IA powers we inspected,[32] we were not satisfied from the records available that associated telecommunications data authorisations were properly made. We suggested agencies seek legal advice. To the extent that any authorisations are determined not to be properly made, we advised agencies to quarantine affected data, determine any use and disclosure implications, and inform partner agencies where applicable.

Demonstrating authorised officer considerations

One of the key matters we assess in reviewing agencies' use of telecommunications data powers is whether the authorised officer had sufficient information to consider the required matters before they make an authorisation, including privacy considerations under s 180F of the Act. In our Office's view, it is clearer for information about authorised officer considerations to be included in contemporaneous documents used by the authorised officer at the time of making the authorisations. Contemporaneous and clear records of authorised officer considerations also satisfy the record-keeping requirements of the Act under s 186A of the Act.

[31] See page 6, above, for an outline of Part 15.
[32] AFP and ACIC.

We made 9 recommendations, 43 suggestions and 10 better practice suggestions across 15 agencies[33] during our 2020–21 inspections in relation to demonstrating authorised officer considerations. These included:

- Increasing the awareness among requesting and authorised officers of the privacy and record-keeping requirements of the Act.
- Implementing measures to ensure requesting and authorised officers consistently document any information, including oral briefings, relevant to the consideration of each authorisation, so authorised officers can demonstrate they considered all relevant matters when authorising access to telecommunications data.
- Supporting authorised officers in accessing relevant information to fulfil their role as decision-makers, including by providing access to all information the authorised officer considers necessary to determine whether the legislative considerations under Chapter 4 of the Act are fully met.
- Incorporating direct guidance in agencies' standard operating procedures and training regarding the record-keeping obligations for authorised officers.
- Establishing quality assurance measures to assess requests made for the disclosure of historic telecommunications data to ensure each request contains sufficient information for an authorised officer to demonstrate they have made the considerations required under s 180F of the Act.

Lack of measures to ensure the recording of authorised officer considerations

Over our last 3 inspections, our Office was not satisfied the AFP clearly demonstrated authorised officers were consistently having regard to all considerations required under the Act. We re-stated our previous recommendation from our 2018–19 report: that the AFP implement processes to ensure authorised officers consistently document any information relevant to considering and approving a telecommunications data authorisation under Chapter 4 of the Act to demonstrate the authorised officer considered all relevant matters, in line with the record-keeping requirements under s 186A(1)(a)(i) of the Act.

While the AFP implemented some changes, during our 2020–21 inspection we identified that in most records inspected there was insufficient information recorded to satisfy us that the authorised officer demonstrated their regard for the considerations required under the Act when making the authorisation. These issues largely resulted from an over-reliance on template wording, a lack of documentation of the individual authorised officer considerations, combined with insufficient background information on the request form to substantiate the request for telecommunications data.

[33] ACLEI, the ACIC, the AFP, ASIC, the CCC WA, the CCC QLD, the Department, IBAC, LECC, the NSW CC, the NT Police, the SA Police, Tasmania Police, Victoria Police, and the WA Police.

We were not yet satisfied the AFP had sufficient measures in place for sustained and consistent improvement across the agency. We recommended the AFP:

- implement measures to ensure authorised officers consistently document information relevant to their consideration and approval of a telecommunications data authorisation to demonstrate they took into account all relevant matters. Where verbal briefings take place or the authorised officer refers to information outside of the request form when making a decision, authorised officers must make contemporaneous notes to ensure that the AFP is able to meet its record-keeping obligation under s 186A(1)(a)(i) of the Act. The mechanism through which this occurs must be consistent across the AFP, and readily available for inspection.
- provide clear guidance to requesting officers to include sufficient information in requests for telecommunications data to enable an authorised officer to appropriately consider a request for telecommunications data in line with Chapter 4 of the Act.

In response, the AFP noted it has created new forms for requests made under Chapter 4 of the Act that prompt requesting officers to address each of the requirements separately with a mandatory field for authorised officer considerations. The AFP also advised it would update its training package, guidance material and undertake education and awareness raising with its staff.

Insufficient information to demonstrate authorised officer considerations

During our 2020–21 inspection of Victoria Police, consistent with the 2 previous inspections we found that most historic authorisation records inspected did not contain sufficient information to demonstrate authorised officers had regard for all required considerations under s 180F of the Act. Victoria Police informed our Office that for 2 of its 3 areas using telecommunications data powers, documents containing information about the reason for an authorisation were destroyed after authorisations were sent to the carrier.

We recommended Victoria Police implement processes to ensure authorised officers consistently document any information relevant to considering and making a telecommunications data authorisation. This includes demonstrating the authorised officer considered all relevant matters in line with the s 180F and the record-keeping requirements under ss 186A(1)(a)(i) and 186A(3) of the Act.

We also suggested that Victoria Police ensure:

- requesting officers are aware of the requirements of the Act and their role in providing relevant information to enable an authorised officer to have full regard for all required considerations
- supporting documentation is kept with each authorisation to confirm the information the authorised officer had regard to in making the necessary

privacy considerations and to support compliance with its record-keeping obligations under ss 186A(1)(a)(i) and 186A(3) of the Act.

In response Victoria Police advised it established a project team to oversee and implement the recommendations, suggestions, and better practice suggestions from our report.

Insufficient records demonstrating authorised officer considerations

During our previous inspection at the ACIC, we found that generally records did not sufficiently demonstrate authorised officers having regard for the considerations required under s 180F of the Act. We suggested the ACIC implement processes to ensure authorised officers consistently demonstrate their regard for required considerations when making a telecommunications data authorisation, in line with the record-keeping requirements of s 186A(1)(a)(i) of the Act. During our 2020–21 inspection, we considered the ACIC was yet to take sufficient action in response to this suggestion.

We continued to identify instances where the ACIC's records contained insufficient information on the particulars of a request for the authorised officer to be satisfied of the matters stipulated by the Act. We reiterated our suggestion from our previous inspection that the ACIC implement processes to ensure requesting and authorising officers consistently document any information relevant to considering and approving an authorisation. We also suggested the ACIC ensure contemporaneous and accurate information is provided in requests, and the ACIC review its multiple authorisation process to ensure authorisations sufficiently demonstrate each disclosure is justifiable and proportionate.

In response, the ACIC acknowledged this finding and advised of action it would take including to increase staff awareness, implement quality assurance processes and strengthen processes.

Data vetting and quality control frameworks

Carriers sometimes provide agencies with telecommunications data that was not authorised for disclosure. Our observation is this is usually inadvertent or due to a carrier 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, they are nevertheless responsible for ensuring this type of data is managed appropriately. Any telecommunications data received outside the parameters of the authorisation should be quarantined from use and disclosure.

Data vetting involves agencies assessing the information and/or documents received from a carrier (the telecommunications data) against what was authorised, to ensure the agency only receives data that was authorised.[34] 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 which have poor, or no data vetting procedures tend to have a higher rate of compliance issues related to receiving data outside the parameters of an authorisation. Our Office considers it essential that all agencies have formal processes, policies, and training in place for vetting and managing telecommunications data.

We found that agencies displaying an effective data vetting and quality control framework, had in place a combination of the following measures:

- A centralised compliance team vetting, and managing all telecommunications data received from carriers prior to disseminating to investigators.
- Detailed guidance material around for vetting, identifying, and managing all telecommunications data received.
- Training for compliance staff in all aspects of data vetting, quarantining and management.

During our 2020–21 inspections, we found that most agencies received data outside the parameters of an authorisation. While generally agencies exercised some form of quality assurance (QA) checks, many agencies lacked formalised QA processes and established guidance to vet incoming telecommunications data comprehensively and consistently and appropriately manage data. We made 2 recommendations, 18 suggestions and 9 better practice suggestions regarding data vetting and quality assurance processes across 15 agencies.[35] These ranged from establishing comprehensive and consistent procedures, formalising existing practices in policy and guidance material, strengthening existing processes or amending to address gaps, and limiting access to quarantined data.

Data vetting guidance material

Over several previous inspections of Tasmania Police, we made findings about data it received outside the parameters of authorisations that were not identified and quarantined. We previously made suggestions to Tasmania Police regarding establishing data vetting and quarantining policies and procedures.

During our 2020–21 inspection, we were pleased to see that Tasmania Police developed procedures for data vetting in line with our previous findings. We will

[34] See Appendix A for further information about how we assess that telecommunications data disclosed by the carrier, and used by the agency, complies with the authorisation.
[35] ACLEI, the ACCC, the AFP, ASIC, the CCC QLD, the Department, IBAC, the ICAC NSW, the NSW Police, the NT Police, the QPS, the SA Police, Tasmania Police, Victoria Police, the WA Police.

continue to assess the effectiveness of these procedures at future inspections, noting the guidance to be provided to investigators on vetting telecommunications data will be included in a training package that was yet to be delivered.

We did not identify any further instances of prospective data outside of the parameters of the authorisations reviewed at this inspection. We identified 7 instances where the telecommunications data disclosed by the carrier was outside the parameters of historic authorisations. In addition to recommending Tasmania Police quarantine specific instances identified, as a matter of better practice we suggested that Tasmania Police make guidance material on data vetting available to investigators as a priority.

In response Tasmania Police advised that it has developed data vetting procedures and incorporated data vetting into a training package, which have been made available to officers.

Lack of formalised data vetting processes

The IBAC does not have a centralised data vetting process when receiving historic data, relying on individual requesting officers to vet disclosures from carriers in the first instance. Requesting officers undertake vetting with informal instructions and no overarching policy or written guidance on how to vet or manage telecommunications data received from a carrier. We note the IBAC is a relatively small agency with a corresponding relatively small number of requesting and authorised officers.

IBAC was identifying several compliance issues through retrospective internal compliance audits completed each month. While this is a good practice, this revealed that vetting processes when the data is disclosed by carriers were not consistently identifying all issues with data received. Enhanced data vetting procedures would limit unnecessary use and disclosure in the first instance which we consider more effective than retrospective audits identifying such issues subsequently.

We suggested the IBAC develop policy and guidance material on how to identify and manage telecommunications data to assist identifying data outside the parameters of an authorisation, and how to quarantine such data appropriately.

The IBAC advised it would consider an appropriate policy position to incorporate into updated guidance material available to requesting officers drawing on matters identified in our inspection reports and would continue the retrospective audits as an auxiliary measure to strengthen and support data vetting by requesting officers. The IBAC also advised it would look to include this matter in information sessions delivered to requesting officers.

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 employer, and
- a purpose of the agency is to identify a 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.

During our inspections we review an agency's processes and controls regarding the special provisions for journalists under the Act, covering:

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

During our 2020–21 inspections we made 2 recommendations, 10 suggestions and 12 better practice suggestions in relation to JIW controls across 16 agencies.[36] While many agencies were aware of the JIW requirements, we identified several gaps in guidance material 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. It is our Office's view that both requesting and authorised officers should be required to actively turn their mind to whether a purpose of making the request is to identify a possible source of a journalist or a journalist's employer.

Insufficient contemporaneous information on whether JIW requirements were considered

At the CCC QLD we identified an inconsistent approach to keeping records related to whether s 180H of the Act may be applicable. This included instances where authorised officers did not leave any comments detailing any consideration as to whether s 180H of the Act may be applicable.

[36] ACLEI, the ACIC, the AFP, ASIC, the CCC QLD, the Department, IBAC, the ICAC NSW, LECC (we note that the LECC did not accept our finding here), the NSW CC, the NSW Police, the NT Police, the QPS, Tasmania Police, Victoria Police and the WA Police.

We were satisfied from our review of the records that the authorisations did not relate to the disclosure of information or documents relating to a person known or believed to be a journalist or an employer of a journalist. However, in some instances we were unable to assess whether s 180H of the Act was appropriately considered by the authorised officer at the time of their decision to make an authorisation.

In addition, we provided a separate JIW report detailing the findings of our review of the CCC QLD's exercise of the special provisions regarding journalists under the Act and associated legislative requirements. We suggested to the CCC QLD that when it is making an authorisation linked to a journalist (or someone who may be a journalist), it seeks legal advice to confirm whether a JIW is required and keeps contemporaneous and comprehensive records of that advice. We also suggested that where it is determined a JIW will not be applied for and an authorisation is to be made, authorised officers should maintain contemporaneous and comprehensive records on what considerations they made upon receipt of legal advice.

In response, the CCC QLD agreed that legal advice should be sought where it is possible the request may relate to a journalist and undertook to update its procedures and training.

Prompts for officers to consider JIW requirements under s 180H of the Act

The CCC QLD's request form and authorisation template included hidden text providing instructions to officers if data being requested is known or reasonably believed to be related to a journalist or journalist's employer. As this hidden text may be removed when the requesting officer enters in the details of the request, we were concerned it would not consistently serve as a prompt for the authorised officer to consider the possible requirement for a JIW under s 180H of the Act.

The CCC QLD subsequently advised it amended its template to make the hidden text available on the form, and that authorised officers are required to acknowledge they considered and are satisfied the authorisation 'is not in relation to' a JIW. We suggested the CCC QLD amend this field to require authorised officers to confirm whether the request relates to a journalist or their employer and whether they have turned their minds to the requirements under s 180H of the Act. As a matter of better practice, we also suggested the CCC QLD include a field on its request form for requesting officers to confirm they turned their mind to whether the request relates to a journalist.

In response, the CCC QLD advised it updated its telecommunications data templates and will provide further training to officers.

Maintaining records to demonstrate JIW considerations

At our 2019–20 inspection we identified a record indicating Tasmania Police may have accessed the telecommunications data of a person who could be a journalist, without having sufficient regard to the requirements of the Act.

Before our 2020–21 inspection we requested and assessed further information about this matter from Tasmania Police. Upon review, we were satisfied Tasmania Police had not breached the JIW provisions. However, we concluded the actions taken by Tasmania Police were not sufficient to manage the risk that telecommunications data would be accessed without a JIW in place when one is required. Amongst other things, we found that Tasmania Police was unable to provide records that demonstrated requesting and authorised officers had sufficient regard to JIW considerations before telecommunications data was requested and accessed. Based on records made available to us, we are not satisfied that requesting and authorised officers considered s 180H of the Act before Tasmania Police accessed telecommunications data in several instances.

During our 2020–21 inspection, we saw some improvement including that Tasmania Police were identifying the need to actively engage with s 180H of the Act. In a separate JIW report we made 4 suggestions to Tasmania Police to assist in further demonstrating compliance and to mitigate risk of non-compliance with the JIW provisions in the Act, including that Tasmania Police:

- increase awareness of the JIW provisions within its cohort of investigators and authorised officers through training
- revise its policies and practices as well as their systems and templates to build in a prompt for officers to consider if a JIW is required and, where there is any connection to journalism, a field to record their considerations
- informed by legal and policy advice (Department of Home Affairs), provide better guidance to their officers about the practical application of the term 'working in a professional capacity as a journalist'
- clearly establish in policy and guidance, for the requirement to seek legal advice if there is any uncertainty as to whether a person may be considered a journalist or a JIW is required.

Tasmania Police advised that it has conducted in person sessions with officers shortly after our inspection to increase awareness of JIW provisions. Tasmania Police also advised that JIW provisions have been included in its training package, standard operation procedures have been amended and guidance has been made available to officers. Tasmania Police also intends to seek advice from the agency administering the legislation as suggested by our Office.

Lack of consistent JIW guidance and awareness for staff

Our 2019–20 inspection identified differing levels of awareness of, and limited guidance about, JIW requirements across areas of the NT Police. We suggested the NT Police develop consistent guidelines regarding the JIW provisions for its staff and make these widely available and incorporate a prompt within requests requiring the requesting and authorising officers to actively consider these requirements.

During our 2020–21 inspection we found that, although the NT Police created a draft JIW application process, it did not implement broader procedural changes to raise awareness or cause requesting and authorised officers to consider whether a request related to a journalist. No authorisation records inspected by our Office demonstrated active deliberation by the requesting or authorised officer of JIW considerations. We could not be satisfied NT Police had sufficient measures in place to ensure it actively considers the application of s 180H of the Act.

We recommended the NT Police, as a matter of priority, develop guidelines addressing the JIW provisions in s 180H of the Act and implement prompts requiring requesting and authorising officers to consider whether a request relates to a journalist or their employer. We suggested as a matter of best practice that NT Police JIW guidance require that legal advice be sought where they identify that a request for telecommunications data access may relate to a journalist or their employer.

In response, the NT Police advised they are addressing our recommendations.

Use and disclosure record-keeping obligations

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

Across 13 agencies[37] inspected in the 2020–21 inspection period, we made 18 suggestions and 5 better practice suggestions regarding use and disclosure record-keeping obligations. These included:

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

[37] ACLEI, the ACIC, the AFP, ASIC, the Department, IBAC, the ICAC NSW, the ICAC SA, the NSW Police, the NT Police, the SA Police, Tasmania Police and Victoria Police.

Insufficient mechanism for recording use or disclosure of telecommunications data

We found the AFP did not have a consistent practice for recording use and disclosure of telecommunications data. Its guidance material states an AFP member responsible for a use or disclosure is required to maintain records of the date and time of use or disclosure with a brief note of the reasons for doing so. However, this can be achieved several ways including official diaries, file notes, electronic or manual logs, email correspondence and in affidavits.

Our Office undertook random spot checks to confirm whether use and disclosure records were being kept. In 2 instances the AFP informed us there were insufficient records to confirm whether the information was used or disclosed. As such, our Office could not be satisfied the AFP had met its record-keeping obligations.

We suggested the AFP implement a single consistent mechanism for recording use or disclosure of telecommunications data that is communicated to all officers who may handle accessed telecommunications data. The AFP advised it would demonstrate action in response to our suggestions at our next inspection.

Lack of awareness for staff of the use and disclosure record-keeping requirements

Following our 2018–19 inspection we suggested Victoria Police include warnings or prompts in its system to remind officers of use and disclosure requirements under the Act. While Victoria Police started to implement our suggestion, this action was still incomplete at our 2019–20 inspection due to IT vendor issues. As an interim measure, Victoria Police emailed a high usage area reminding them of their use and disclosure obligations.

At our 2020–21 inspection, Victoria Police advised the update to the system was yet to occur. Victoria Police advised our Office that it is the responsibility of each individual officer receiving telecommunications data to maintain records of use and disclosure. However, we found no guidance material available to promote consistency in the detail and manner of record-keeping by individual officers. We were unable to assess compliance with use or disclosure requirements in 2 of the 3 areas of Victoria Police that use these powers.

We suggested Victoria Police implement further measures to improve awareness of the use and disclosure obligations as well as record-keeping requirements. As a matter of better practice, we also suggested Victoria Police consider additional guidance to facilitate consistent use and disclosure record-keeping, and to ensure all records are available for future inspections.

In response, Victoria Police advised it established a project team to oversee and implement the recommendations, suggestions, and better practice suggestions from our report.

Training and guidance material for officers

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.

Where we identified a systemic problem, a key contributing factor across agencies was a lack of detailed and practical guidance material (including training), or a lack of detailed and documented administrative processes, regarding authorisation requirements and access to telecommunication data. Agencies without 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 13 recommendations, 80 suggestions, and 23 better practice suggestions across all agencies in relation to training, guidance and support for officers involved in requesting, authorising, using, and managing telecommunications data. This included the need for:

- mandatory and ongoing training
- sufficient standard operating procedures and guidance material, and
- embedded guidance and first line advice for officers.

Limited guidance material available for staff

Only limited guidance on Chapter 4 of the Act was available for officers of the NT Police, within the request and application workflows. While the NT Police was developing a standard operating procedure (SOP) on access to telecommunications data, this was not finalised at the time of our inspection, and we understood it was only available to members in one area.

We did not consider the available templates or workflows provided sufficient practical guidance to NT Police officers on the matters which require consideration for telecommunications data authorisations. The material largely focused on authorisation workflow processes, rather than legislative compliance.

While the NT Police delivers annual training to detectives, this does not capture the cohort of all requesting officers and authorised officers. A lack of training can directly impact on the ability of officers to understand the legislative framework, and this affects agency compliance.

The legislative obligations and considerations to be weighed are complex. We do not consider NT Police authorised officers are adequately supported in their decision-making. This is because there are no supporting purpose-made guidance materials, specific policy or clear procedures around the relevant thresholds and legislative considerations. Some officers involved in the exercise of these powers do not have training available to them. The absence of detailed guidance material and training presents risks to the NT Police including for compliance and continuity of corporate knowledge.

We recommended that, to improve compliance with Chapter 4 of the Act, the NT Police should:

- prioritise the finalisation of its SOP on accessing telecommunications data
- ensure the SOP provides clear guidance setting out the obligations of members accessing these powers
- ensure the guidance is easily accessible to all officers using these powers
- expand its annual training to cover the full cohort of officers involved in the exercise of these powers.

In response, the NT Police advised our recommendations were being addressed.

Inconsistency regarding practices and administration of the telecommunications data regime

The SA Police's processes in relation to telecommunications data powers evolved at a team-level without a comprehensive agency-wide review of the administration of the regime, or unified guidelines on its administration. This created inconsistency between business areas regarding practices and administration of the telecommunications data regime. This also prevented the SA Police from consistently addressing findings from our previous inspection reports.

We were not satisfied there was sufficient guidance available to requesting officers to support the SA Police's compliance with legislative obligations and decision-making criteria. We noted the online telecommunications data training package at SA Police had a low completion rate within the relevant records period.

We recommended the SA Police develop a whole-of-agency governance framework for accesses to telecommunications data to establish clear policy and guidelines on compliance obligations for members accessing telecommunications data, procedures for requesting, authorising, and managing telecommunications data, and authorisation templates for each type of authorisation. We also suggested the SA Police provide clear guidance and training to ensure requesting and processing officers are aware of their obligations under Chapter 4 of the Act.

In response, the SA Police advised it has established a governance committee responsible for addressing issues identified through inspections and overseeing the development and implementation of appropriate policy, procedures, training and periodic compliance auditing; developed and implemented corporate policy and a new Standard Operating Procedure; and reviewed and developed a new online training package. The SA Police also advised that it is forming working groups to develop and implement standardised request and authorisation templates, training and reporting platforms for use across the SA Police.

Finalisation of guidance material and staff awareness

In our 2019–20 inspection report we recommended the Department of Home Affairs prioritise finalising and implementing its draft policy statement and procedural instruction regarding Chapter 4 of the Act, and ensure these documents provide sufficient guidance on the obligations of authorised officers. We recommended the Department provide additional guidance material to those performing the role of authorised officer and implement training to support decision-making and increased awareness of legislative obligations under Chapter 4 of the Act. The Department accepted these recommendations.

During our 2020–21 inspection we found that while the Department progressed its policy statement and procedural instruction through clearance processes, these documents were not finalised. Before we finalised our report, the Department advised that one policy statement had since been finalised. Our Office considers the lack of a full suite of finalised guidance materials directly impacts authorised officers' ability to confidently navigate legislative requirements and presents considerable risks to continuity of corporate knowledge. Our concern was amplified due to the small cohort of authorised officers at the department and the practice of having short-term authorised officer acting positions. We again emphasised the importance of finalising these processes in our report.

In response, the Department advised that its procedural instructions and standard operating procedures for requesting and authorising officers are in final stages of consultation, and its legal area conducted training and refresher sessions for relevant teams shortly after our inspection.

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

In some instances, carriers may provide additional information that an agency did not specifically authorise. 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	0491 570 006[38]
Authorised Data	Call charge records
Period Authorised	1/07/2018 to 30/06/2019
Date Authorised	30/06/2019 1300 (AEST)
Sent to Carrier	30/06/2019 1400 (AEST)

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

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

Our Assessment	
1	This line is within the parameters of the authorisation as conversion from UTC to AEST means this call occurred at 01/07/2018 0700 AEST. NB: as the authorisation does not state a time zone for the period authorised, it is taken to apply the time zone of the location in which it was made.
2	This line is within the parameters authorised.
3	This line is not authorised, as the authorisation only related to calls made by the mobile phone number, not calls received by this number.
10	This line is authorised, as after conversion to AEST, it occurred at 30/06/2019 1559, being before the time the authorisation was notified to the carrier.
11	This line is not authorised, as it is dated after the time the authorisation was notified to the carrier.
For these results, it would be our expectation the agency was able to proactively identify and quarantine this data (lines 3 and 11) before results were disseminated to an investigator. Where this unauthorised information is not identified before being sent to investigators, we suggest the agency contact any recipients and quarantine the data. We would also suggest the agency ascertain whether use or disclosure took place.	

Appendix B – 2020–21 Stored communications and telecommunications data inspection schedule

Agency	Inspection type	Inspection Start Date	Inspection Finish Date
CCC QLD	Stored Communications	13-Jul-2020	15-Jul-2020
ACLEI	Telecommunications Data	13-Jul-2020	17-Jul-2020
ACCC	Stored Communications & Telecommunications Data	28-Jul-2020	31-Jul-2020
QPS	Stored Communications	03-Aug-2020	07-Aug-2020
ACIC	Stored Communications	07-Sep-2020	11-Sep-2020
ACLEI	Stored Communications	09-Sep-2020	10-Sep-2020
CCC QLD	Telecommunications Data	21-Sep-2020	25-Sep-2020
NSW PF	Telecommunications Data	28-Sep-2020	02-Oct-2020
CCC WA	Stored Communications & Telecommunications Data	29-Sep-2020	02-Oct-2020
LECC	Telecommunications Data	12-Oct-2020	16-Oct-2020
ICAC SA	Stored Communications & Telecommunications Data	13-Oct-2020	15-Oct-2020
IBAC	Stored Communications	04-Nov-2020	05-Nov-2020
SA Police	Stored Communications	04-Nov-2020	06-Nov-2020
WA Police	Telecommunications Data	23-Nov-2020	27-Nov-2020
ASIC	Telecommunications Data	07-Dec-2020	09-Dec-2020
The Department	Telecommunications Data	07-Dec-2020	11-Dec-2020
IBAC (2019-20)	Telecommunications Data	16-Mar-2020	05-Nov-2020[39]
IBAC (2020-21)	Telecommunications Data	11-Jan-2021	14-Jan-2021
AFP	Stored Communications	18-Jan-2021	22-Jan-2021
ICAC NSW	Stored Communications & Telecommunications Data	27-Jan-2021	29-Jan-2021
SA Police	Telecommunications Data	01-Feb-2021	05-Feb-2021
The Department	Stored Communications	08-Feb-2021	10-Feb-2021
ACIC	Telecommunications Data	08-Feb-2021	12-Feb-2021
AFP	Telecommunications Data	15-Feb-2021	26-Feb-2021
NSW CC	Stored Communications & Telecommunications Data	22-Feb-2021	25-Feb-2021
LECC	Stored Communications	15-Mar-2021	19-Mar-2021
QPS	Telecommunications Data	22-Mar-2021	26-Mar-2021
WA Police	Stored Communications	06-Apr-2021	09-Apr-2021
Tasmania Police	Stored Communications & Telecommunications Data	12-Apr-2021	16-Apr-2021
Victoria Police	Stored Communications	03-May-2021	07-May-2021

[39] Our inspection of IBAC for the periods 01 July 2017 to 30 June 2018 and 01 July 2018 to 30 June 2019 commenced in March 2020 but was paused due to the COVID-19 pandemic, the remainder of the inspection was conducted in November 2020.

Agency	Inspection type	Inspection Start Date	Inspection Finish Date
NT Police	Stored Communications & Telecommunications Data	17-May-2021	21-May-2021
NSW PF	Stored Communications	31-May-2021	04-Jun-2021
Victoria Police	Telecommunications Data	05-Jul-2021	09-Jul-2021

Appendix C – Stored communications inspection criteria 2020–21

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 2020–21

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

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

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

Process checks

- Does the agency have effective procedures in place to ensure that authorisations are properly applied for, and are they sufficient?
- Does the agency have effective controls, guidance and 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 in s 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 – 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 to enforcement agencies. *Historic authorisation*s Agencies may authorise the disclosure of specified information or documents that came into existence before a carrier receives notification of an authorisation. Historic authorisations can be made

Term (and section of the Act)	Description
	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 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 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.
(Telecommunication service) carriers	Carriers and carriage service providers who supply certain carriage services over a telecommunications network. Carriers in Australia include but are not limited to: • Telstra Corporation Ltd • Singtel Optus Pty Ltd • Vodafone Hutchison Australia Pty Ltd.
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.

Term (and section of the Act)	Description
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.
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'.

Term (and section of the Act)	Description
	While the Act does not define 'forthwith' an agency may hold itself to a particular timeframe which will guide our assessments. However, we will also consider whether this timeframe is reasonable in the circumstances noting the ordinary definition of 'forthwith' as immediate and without delay. Where an agency does not have a strict timeframe for destructions, in assessing compliance with this provision, our Office makes an assessment based on our understanding of an agency's policies and procedures and what we consider to be reasonable in the circumstances.
Disclosure by agencies to the Office	Prior to or during an inspection, agencies may make a disclosure to our Office outlining 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.

Term (and section of the Act)	Description
Inspection report	An inspection report presents the findings of an inspection together with any suggestions or recommendations made in response to findings. An inspections report may be formal or streamlined. We prepare formal reports where our inspection identified significant or systemic issues or where we consider a formal recommendation is warranted to address legislative non-compliance. Formal reports are generally signed by the Ombudsman and sent directly to an agency's chief officer for action and response. These inspection reports and any subsequent comments on the reports from agencies, contribute to this annual report to the Minister. We prepare streamlined reports when our inspection findings are not indicative of significant or systemic issues. The instances of non-compliance reported in streamlined reports are typically 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

Term (and section of the Act)	Description
	• 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.
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

Term (and section of the Act)	Description
	period during which time the agency may obtain a warrant to access those communications. There are 2 types of preservation notices: • Domestic preservation notices • Foreign preservation notices <u>Domestic preservation notices</u> • Historic domestic preservation notice – may be given by a criminal law-enforcement agency. These notices require carriers to preserve stored communications it holds at any time on or before the day the carrier receives the notice. • Ongoing domestic preservation notice – may only be given by a criminal law-enforcement agency that is also an interception agency. These notices require carriers to preserve stored communications it holds at any time from when the carrier receives the notice to 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

Term (and section of the Act)	Description
	• the seriousness of any protection of the public revenue in relation to which the authorisation is sought • whether the authorisation is sought for the purposes of finding a missing person • the likely relevance and usefulness of the information or documents • the reason why the disclosure or use concerned is proposed to be authorised.
Prospective authorisation s 180	A prospective authorisation enables access to information or documents that come into existence when an authorisation is in force. A prospective authorisation may also authorise the disclosure of 'historic' data – telecommunications data that came into existence before the time the authorisation comes into force. Authorised officers must not make a prospective authorisation unless the disclosure is reasonably necessary for investigating a serious offence or an offence against the law of the Commonwealth, a State or Territory that is punishable by imprisonment for at least 3 years. Prospective authorisations come into force when a person (usually a carrier) receives notification of the authorisation. Unless the authorisation is revoked earlier or is an authorisation made under a 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:

Term (and section of the Act)	Description
	• Storing the information on a separate disc and locking the disc away from investigators • Copying the information to a separate password protected file accessible only to nominated officers • Other actions in line with agency policies and procedures.
Receiving stored communications information s 135	Section 135(2) of the Act states the chief officer of a criminal law-enforcement agency may authorise in writing officers or classes of officers, 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

Term (and section of the Act)	Description
	decides not to apply for a warrant to access the preserved stored communications. A domestic preservation notice is revoked by the issuing agency giving the carrier to whom it was given written notice of the revocation. Mandatory revocation provisions for foreign preservation notices given by the AFP are outlined under s 107R of the Act. An agency may also revoke a preservation notice at any time at its own discretion (s 107L(1) of the Act). <u>Stored communications warrants</u> 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.
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	A person who rents or uses a telecommunications service.

Term (and section of the Act)	Description
s 5	
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.
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.

Term (and section of the Act)	Description
	'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.