COMMONWEALTH OMBUDSMAN

A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979*

For the period 1 July 2015 to 30 June 2016

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

March 2017

COMMONWEALTH OMBUDSMAN

A report on the Commonwealth Ombudsman's monitoring of agency access to stored communications and telecommunications data under Chapters 3 and 4 of the *Telecommunications (Interception and Access) Act 1979*

For the period 1 July 2015 to 30 June 2016

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

March 2017

ISSN 2207-4686

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

Table of Contents

Executive summary

This report presents the results of inspections conducted by the Commonwealth Ombudsman under s 186B of the *Telecommunications (Interception and Access) Act 1979* (the Act) from 1 July 2015 to 30 June 2016.

Under the Act, 20 specified law enforcement agencies are able to lawfully access individual's telecommunications data and/or stored communications when investigating certain offences.

Telecommunications data, or 'metadata', is information about a communication. Metadata does not include the contents of a communication. In the example of a phone call, metadata may include the phone numbers of the two parties to the conversation, the duration, date and time of that phone call but not what was said. Any of the 20 specified agencies have the power to authorise access to this information. If, however, an agency wishes to access metadata that will identify a journalist's information source, the agency must apply to an external issuing authority for a warrant.

Stored communications are communications that have already occurred and are stored on a carrier's systems. An example of this would be a Short Messaging Service (SMS) that has been sent to or from a person's mobile phone, and would include the contents of that message. An agency must apply to an external issuing authority for a warrant to access stored communications.

Before a warrant is issued, however, an agency may authorise the 'preservation' of a stored communication, to prevent a carrier from destroying the communication before it can be accessed under a warrant.

These are covert and intrusive powers, given to agencies for the purposes of combating crime and protecting our community.

The fact that these powers are exercised covertly is the reason why oversight is so important. A person who has been subject to the powers will not be aware of the fact, and therefore, will not be in a position to make a complaint. Instead, the Ombudsman provides independent oversight by conducting inspections at each agency that has exercised these powers. At these inspections, we assess whether agencies are compliant with legislation and whether they have used these powers in line with the spirit of the legislation.

The purpose of oversight is to provide assurance to Parliament and the wider public that agencies are using these powers as Parliament intended. That is, that these powers are not being abused and that agencies are being held accountable for their use. We report our findings to agencies and the Commonwealth Attorney General, who must then make the report public.

It is reassuring to note that overall, agencies are appropriately exercising their powers to access stored communications and have frameworks in place to ensure appropriate access to metadata. It was evident that agencies are committed to compliance and want to 'get it right'.

During an inspection, there may be a range of issues identified, including minor administrative errors, instances of serious non-compliance and systemic issues. The Ombudsman may make suggestions for improvement or may make formal recommendations in instances where an issue has not been addressed by the agency, or if it is sufficiently serious. Of the 36 inspections conducted under the Act during 2015-16, only three recommendations were made. Ultimately, all agencies have been responsive to the Ombudsman's findings.

Access to metadata

Overseeing access to metadata is a new function for the Ombudsman. Agencies have accessed metadata for a number of years without external oversight, which means that each agency already had policies and procedures in place.

As this was the first time agencies would be scrutinised on how they managed and used this power, during 2015-16 the Ombudsman focused on understanding the policies and procedures already in place at each agency. Due to the varying size, structure, nature and complexity of each agency, processes varied. In taking all of this into account, we were able to work with each agency to identify individual strengths and risks for non-compliance with the Act.

As a result of our 2015-16 inspections, we found that agencies had mostly sound policies and procedures in place for accessing metadata. Although each agency faced its own challenges, we identified some common areas of risk for all agencies, including:

- the level of involvement and support from senior leadership
- the timeliness and comprehensiveness of training given to those exercising metadata powers
- the effectiveness of internal communications within an agency to raise awareness of relevant changes and share best practices.

Overall, agencies demonstrated a strong commitment to comply with the Act. Agencies were open to feedback and willing to improve their processes. This was particularly evident in the lead-up to inspections, with significant engagement from most agencies with the Ombudsman.

Access to stored communications

The Ombudsman has performed an oversight role in relation to access to stored communications since 2006. This is the Ombudsman's first public report on the results of these inspections.

As a result of the 2015-16 inspections, most agencies were compliant with the Act. However, we identified non-compliances in relation to various record keeping provisions and adherence to warrant conditions and restrictions. All agencies were ultimately receptive to our current and previous findings and best practice suggestions.

Introduction

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act* 2015 (Data Retention Act) commenced on 13 October 2015, giving the Commonwealth Ombudsman (the Ombudsman) an over-arching role in assessing agency compliance with both Chapters 3 (preserving and accessing stored communications) and 4 (accessing metadata) of the Act.[1]

The Ombudsman is required to inspect agency records in order to determine the extent of compliance in the use of these powers by the agency and its officers. The Ombudsman is also required to report to the Commonwealth Attorney-General (the Minister) on the results of those inspections. The Minister must then table this report in Parliament.

Access to stored communications and metadata are intrusive powers afforded to agencies. The Ombudsman's role is to independently assess compliance with legislation and provide assurance to the Parliament and wider public that agencies are using these powers as they were intended. In this way, we can improve transparency around how these powers are exercised, the level of legislative compliance being achieved and the safeguards in place to ensure that these powers are appropriately managed.

Prior to the Data Retention Act, agencies could lawfully obtain metadata from telecommunications carriers, but there was no independent oversight of this power. Neither the Act nor the predecessor arrangements in the *Telecommunications Act 1997* included an independent oversight arrangement in relation to metadata.

In contrast, the Ombudsman has performed an oversight role in relation to stored communications since 2006. This role, however, was limited to assessing compliance with the record keeping and destruction provisions of Chapter 3. The Data Retention Act expanded the Ombudsman's role so that it encompasses the whole of Chapter 3, consistent with the oversight of metadata.

In outlining our role, it is important to note that we do not oversee telecommunications carriers. However, we do liaise with carriers to understand how their practices may impact agency compliance.

Metadata inspections

Chapter 4 of the Act sets out the procedures by which enforcement agencies may access metadata held by a telecommunications carrier. An internally issued

[1] The relevant agencies under the Act are criminal law enforcement agencies for stored communications and enforcement agencies for metadata. These agencies are defined under ss 110A and 176A of the Act respectively.

authorisation enables carriers to lawfully disclose metadata to the agency. In certain circumstances, a journalist information warrant is also required.[2]

During our first round of inspections, we conducted a 'health check' inspection at each of the 20 agencies currently defined as an enforcement agency under s 176A of the Act. This report presents the results of those inspections, which were conducted between 13 October 2015 and 30 June 2016.

The objective of these 'health check' inspections was to assess the health of each enforcement agency's metadata compliance framework and identify areas of compliance risk.

We used the Australian Standard on Compliance Management Systems (AS ISO 19600:2015) to determine whether agencies have adequate policies and procedures in place to ensure ongoing compliance with Chapter 4. Details on the criteria for our metadata inspections can be found at Appendix A.

As a result of our inspections, we have gained a comprehensive understanding of, and conducted thorough analysis on, the policies, procedures and controls in place at each agency. This will be used as a benchmark for future inspections of individual warrants and authorisations.

Stored communications inspections

Chapter 3 of the Act sets out the procedures for criminal law-enforcement agencies to preserve and access stored communications that are held by a telecommunications carrier under the authority of a stored communications warrant. The purpose of preservation is to prevent stored communications from being destroyed before those communications can be accessed under a warrant.[3]

This report presents the results of stored communications inspections conducted by our office at 16 criminal law-enforcement agencies between 1 July 2015 and 30 June 2016. Four agencies defined as criminal law-enforcement agencies under s 110A(1) of the Act advised our office that they did not exercise stored

[2] A journalist information warrant permits an agency to access metadata relating to a particular person (or employer of a person) who is reasonably believed to be working in a professional capacity as a journalist, where the purpose of the access is to identify another person whom the agency knows or reasonably believes to be a source of information for the journalist.

[3] A notice to preserve stored communications is issued by an officer within the agency, while a stored communications warrant is issued by an eligible judge or member of the Administrative Appeals Tribunal.

communications powers during the inspection period.[4] As such, no inspection was conducted at these agencies.

Due to the sensitive nature of the information inspected, part of our risk mitigation strategy is to limit inspections to records relating to warrants that are no longer in force. Our inspections are therefore retrospective in nature. During 2015-16, we assessed records from the period 1 July 2014 to 30 June 2015.[5]

As the stored communications inspections conducted during 2015-16 covered records that had been created prior to the commencement of the Data Retention Act, they were conducted in accordance with 2014-15 inspection methodologies. Likewise, any references in this report to sections from Chapter 3 of the Act refer to the Act in existence at the time the powers were used (prior to 13 October 2015).

The objective of these stored communications inspections was to determine the extent of compliance by an agency with ss 150 (destructions), 150A and 151 (record keeping) of the Act.

We also conducted additional compliance checks which focused on areas of high risk, such as assessing whether the agency is only dealing with lawfully accessed stored communications.[6] These checks strengthen the assurance we can provide to the Parliament and wider public.

It is also worth noting that, in reporting on the results of stored communications inspections, we are constrained by the secrecy provisions in s 133 of the Act. These provisions prohibit the disclosure of certain information.

Details on the criteria for our stored communications inspections can be found at Appendix B.

[4] These agencies were the Australian Securities and Investments Commission, the Corruption and Crime Commission, the Independent Broad-based Anti-corruption Commission and the Independent Commissioner Against Corruption (South Australia).

[5] While we endeavour to inspect all agency records which fall within the relevant inspection period, at agencies with a significant volume of records, a sample size is selected in accordance with Auditing Standard ASA 530 *Audit Sampling*.

[6] Under s 153(3) of the Act, the Ombudsman can report on any contraventions of the Act (other than contraventions of ss 150, 150A or 151) which were noted during stored communications inspections.

Inspection findings

Australian Commission for Law Enforcement Integrity (ACLEI)

Stored communications inspection

We conducted our stored communications inspection of ACLEI on 27 October 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Not assessed at this inspection.[7]
2. Has the agency properly managed accessed information?
Not assessed at this inspection.
3. Has the agency properly applied the preservation notice provisions?
Compliant, with the exception of one instance where an ongoing preservation notice was given when another ongoing preservation notice was already in force with that carrier for the same person, contrary to s 107J(1)(e).[ii] Despite this instance, we are of the view that ACLEI has sufficient procedures in place regarding preservation notices. In particular, we commend ACLEI's process for ensuring that ongoing domestic preservation notices are revoked when the conditions under s 107J(1)(c) and (d) are no longer met.[ii] However, ACLEI's process for giving ongoing domestic preservation notices could be strengthened by embedding a check for whether another ongoing preservation notice is already in force with the same carrier for the same person (or service). If it has not already done so, we suggest that ACLEI amend its standard operating procedures to include such a check.
4. Has the agency satisfied certain record keeping and reporting obligations?
Compliant. We are of the view that ACLEI has sufficient record keeping and reporting practices in place.

[7] ACLEI advised that it had not been issued with any stored communications warrants during the inspection period.

5. Was the agency cooperative and frank?
Compliant. ACLEI has continued to be open and assistive during inspections. We note positively that ACLEI provided us with a detailed overview of the procedures it has in place for giving and revoking preservation notices.

Telecommunications data inspection

We conducted our telecommunications data inspection of ACLEI on 7 April 2016. Our findings against each inspection criterion are as follows.

1. Leadership
ACLEI has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this is underpinned by ACLEI executive's strong commitment to achieving compliance, as demonstrated by their support for increased training in the requirements of Chapter 4. ACLEI executive set the agenda for the agency's induction program, emphasising the importance of compliance in the exercise of the powers.
2. Planning
ACLEI has plans in place to support compliance, which include: compulsory training in the requirements of Chapter 4 for all staff who require access to telecommunications data; an induction program that includes sessions on the requirements of Chapter 4; an onus on those applying for access to telecommunications data to sufficiently address privacy (a new requirement under Chapter 4); and a process to identify circumstances where a journalist information warrant (JIW) may be needed. ACLEI involved relevant areas (the executive, operations support and legal) in the planning stage as part of an informal working group. ACLEI has contacted our office and the Attorney-General's Department with queries regarding compliance with Chapter 4. Representatives of ACLEI's General Counsel and officers involved in exercising these powers and have engaged in 'metadata forums' hosted by our office. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
ACLEI reported that it is compulsory for all officers involved in accessing telecommunications data to receive training in the requirements of Chapter 4. In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations and to conduct ongoing assessment of compliance risks. In addition to the strong support and involvement from its executive, ACLEI's General Counsel and operations support staff have been involved in the planning and establishment of JIW processes at the agency. ACLEI also advised that it has a dedicated legal officer for the Act.

We noted effective communication and awareness-raising within the agency regarding compliance with Chapter 4. This included communication from legal to investigations staff drawing attention to the new requirements for JIWs and privacy considerations, and the timely distribution of updated standard operating procedures (SOPs).

ACLEI demonstrates a strong compliance culture. Information relating to instances of non-compliance is retained by ACLEI and will be self-disclosed at Ombudsman inspections.

4. Operation

The controls ACLEI has in place to support compliance are not automated and rely on the skills, knowledge and experience of staff. For example, the majority of authorisations are completed by one highly experienced authorised officer, the head of ACLEI's operations support area, who is aware of most details relating to investigations. A quality assurance role is also performed by an officer within the operations support area in relation to applications for prospective telecommunications data.

Processes for detecting a need for JIWs are embedded in the templates used to apply for access to telecommunications data. When required, the General Counsel will be engaged to progress an application for a JIW.

ACLEI has comprehensive SOPs on accessing telecommunications data, which are updated as the need arises. These SOPs specifically address the requirements of Chapter 4 and are available to all staff involved in the application process for telecommunications data. Updated SOPs receive approval from the ACLEI Commissioner prior to their release.

5. Performance Evaluation

As with the operation of ACLEI's compliance framework, the processes ACLEI has in place to self-evaluate the effectiveness of its compliance procedures are largely reliant on the knowledge and experience of a limited number of authorised officers, rather than automated processes. For example, while non-approved applications are retained by ACLEI, it is the usual process for the authorised officer to discuss applications lacking in detail with the applicant directly, rather than rejecting an application outright. This process of informal training is the primary means by which ACLEI evaluates its performance and strengthens its level of compliance with Chapter 4.

ACLEI's protocols and governance arrangements are overseen by a governance board and an external audit committee.

Australian Competition and Consumer Commission (ACCC)

Stored communications inspection

We conducted our stored communications inspection of the ACCC on 21 December 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
While the stored communications warrants were lawfully issued, in all instances the authority of the warrant had been exercised by a person not authorised under s 127(1) of the Act.[xi] We note the prompt remedial action taken by the ACCC to address this issue. Two weeks after the issue occurred, the chief officer's authorisation under s 127(2) was updated to cover the person who had exercised the authority of the warrants.
2. Has the agency properly managed accessed information?
Compliant. Nothing came to our attention to suggest that the ACCC had not properly managed accessed information. We are of the view that the ACCC has sufficient procedures in place to manage accessed information.
3. Has the agency properly applied the preservation notice provisions?
Not compliant. In all instances preservation notices given by the ACCC had more than one person specified, which is not provided for under the Act.[i] We note that the ACCC's standard operating procedures state that a domestic preservation notice may only specify one person, however this guidance was not followed in these instances. At the inspection, the ACCC advised that its legal team performs a quality assurance role in relation to stored communications warrant applications. We suggest that the ACCC may wish to extend a quality assurance check to its preservation notices, to reduce the likelihood of this issue occurring in future. We also identified a procedural issue whereby the ACCC gave historic domestic preservation notices, each relating to the same persons, to a carrier on four consecutive days.[8]

[8] There are two kinds of domestic preservation notices:

While this is not in breach of any legislative provision, it could be perceived as achieving the same result as an ongoing domestic preservation notice.[v] Under the Act, only an 'interception agency' may give an ongoing preservation notice. As the ACCC is not an interception agency, it may wish to reconsider this practice moving forward.

In response to these issues, the ACCC advised that it identified and implemented areas for improvement following the inspection and updated its internal procedures accordingly. We will assess the effectiveness of these measures at future inspections.

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

Compliant.

We are of the view that the ACCC has sufficient record keeping and reporting practices in place.

5. Was the agency cooperative and frank?

Compliant. The ACCC has continued to be open and assistive during inspections. In particular, we note positively that the ACCC sought our comment on its standard operating procedures relating to domestic preservation notices and stored communications warrants.

The ACCC advised that this report, and its actions to address areas for improvement, will be exposed to the ACCC governance processes.

- historic domestic preservation notices, which cover stored communications held by the carrier on a particular day, and
- ongoing domestic preservation notices, which cover stored communications held by the carrier in a particular 30-day period.

Telecommunications data inspection

We conducted our inspection of the ACCC on 4 May 2016. Our findings against each inspection criterion are as follows.

1. Leadership
The ACCC has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that senior management have a strong role in the overall compliance framework at the agency. It was also clear that senior management have a good knowledge of the legislative requirements and their responsibilities as authorised officers. As the authorised officer function at the ACCC is restricted to experienced senior managers, we are of the view that this acts as an effective compliance control. During the inspection, senior managers expressed the view that in exercising their powers under Chapter 4 the impact on privacy and proportionality are taken seriously.
2. Planning
The ACCC has plans in place to support compliance. Enhancements have been made to systems to enable compliance to be demonstrated at our future inspections; and all telecommunications data requests pass through the ACCC's governance area prior to consideration by authorised officers. The ACCC involved relevant internal areas in the planning stage, including authorised officers and the governance and legal teams, to produce standard operating procedures (SOPs) on accessing telecommunications data. The governance team is responsible for updating the SOPs when there are changes to the legislation and raising general awareness of legislative requirements across the agency. The ACCC has engaged with our office, the Attorney-General's Department and the Australian Government Solicitor regarding compliance with Chapter 4, and the Chief Operating Officer and staff members involved in exercising powers, and compliance, have engaged in 'metadata forums' hosted by our Office. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
At the time of inspection the ACCC had not yet developed a formal training program on the requirements of Chapter 4. In addition, guidance material available for requesting officers is limited, although detailed SOPs do exist for the governance area, which checks all telecommunications data requests prior to consideration by an authorised officer. The ACCC could improve its overall

compliance framework by developing training and SOPs that specifically target, and are available to, officers seeking to access telecommunications data (which could also be used when inducting new authorised officers).

The lack of training is mitigated by the availability of the ACCC's governance area to provide support to investigators and authorised officers as the subject matter experts for telecommunications data requests.

In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations and to conduct ongoing assessment of compliance risks. Senior management support for and involvement in the compliance framework is strong. Furthermore, legislative changes are monitored by the governance team, which releases intranet 'news flash' communications on telecommunications data in conjunction with the legal team.

We noted effective communication and awareness-raising within the organisation regarding compliance with the new requirements of Chapter 4. This included weekly meetings, briefing notes, intranet announcements, and reinforcement through informal training.

The ACCC demonstrates a strong compliance culture.

4. Operation

Most of the ACCC's compliance controls rely on the skills, knowledge and experience of authorised officers and the governance area for their effectiveness. Despite this, it is our view that the structure of the agency mitigates the risk associated with non-automated controls. In particular, this team acts as an effective additional control as the gatekeeper for all telecommunications data requests, ensuring they comply with the requirements of Chapter 4. During the inspection, we noted strong record keeping practices, skilled and experienced staff, and effective embedded processes. However, the ACCC could improve its processes by raising awareness of monitoring and quarantining procedures for information received from carriers outside the remit of authorisations.

We note the ACCC has a process in place for requesting journalist information warrants, however we suggest that this process is formalised through its inclusion in the SOP's.

5. Performance Evaluation

We noted that there were a number of compliance processes in place to self-evaluate the effectiveness of the ACCC's compliance procedures. These processes include: weekly review meetings between investigators and authorised officers about applications; multiple layers of approval required for telecommunications data requests; and vetting by officers in the governance area.

Remedial Action

In response to the draft report, the ACCC advised that it will be developing actions to address those areas identified for possible improvement, including: targeted training; awareness raising of quarantining procedures for information received from carriers outside of the remit of authorisations; and formalisation of particular matters within the SOPs.

Australian Criminal Intelligence Commission (ACIC)

Stored communications inspection

We conducted our stored communications inspection of the Australian Crime Commission (ACC)[9] from 10 to 12 September 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Not assessed at this inspection.
2. Has the agency properly managed accessed information?
Not assessed at this inspection.
3. Has the agency properly applied the preservation notice provisions?
Compliant, with six instances where we were unable to determine compliance with mandatory revocation requirements under s 107L(2)(a)(ii) of the Act.[iv] Despite these instances, we are of the view that the ACC has sufficient procedures in place regarding preservation notices. We also note that planned enhancements to its compliance database may assist the ACC to prevent this issue from reoccurring. Nevertheless, we suggested that the ACC may wish to amend its request form for preservation notices to remind applicants of the obligation to revoke. In response, the ACC advised that it has amended its preservation notice form accordingly.
4. Has the agency satisfied certain record keeping and reporting obligations?
We were not able to assess the ACC's compliance with ss 150A and 151 of the Act, which are the record-keeping provisions in relation to stored communications.[xv] Though the ACC had been issued with five stored communications warrants during the inspection period, these records were not presented to our office for examination at the inspection. The warrants had not been executed, and the relevant stored communications were instead accessed under corresponding telecommunications interception warrants. This contributed to a misunderstanding

[9] The Australian Crime Commission merged with CrimTrac to form the Australian Criminal Intelligence Commission from 1 July 2016. As the Australian Crime Commission was still an entity at the time of our inspection, we have referred to it as such for the purpose of this report.

at the inspection that the ACC had only been issued with telecommunications interception warrants during the inspection period.

In addition, six preservation notices were not presented to our office for examination at the inspection due to an administrative oversight.

The ACC presented these records to our office at the subsequent inspection held in July 2016, the results of which will be reported on at the end of the 2016-17 inspection period.

In our view, this oversight is an outlier which is not representative of the ACC's general record-keeping practices.

5. Was the agency cooperative and frank?

Compliant. The ACC has continued to be open and assistive during inspections.

We also appreciate the informative opening briefing the ACC prepares for each inspection, in which compliance issues and procedural updates which have occurred since the previous inspection are disclosed.

Telecommunications data inspection

We conducted our inspection of the ACC on 9 November 2015. Our findings against each inspection criterion are as follows.

1. Leadership
The ACC has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this was underpinned by the ACC executive's strong commitment to achieving compliance. For example, the executive was involved in a training seminar for authorised officers, emphasising the importance of personal accountability.
2. Planning
The ACC has plans in place to support compliance, which include: an onus on those applying for access to telecommunications data to sufficiently address privacy (a new requirement under Chapter 4), a process for capturing disclosures of telecommunications data to other agencies; an online system to guide officers through the disclosure process and journalist information warrant (JIW) prompts in the templates for requesting and authorising access to prospective telecommunications data. The ACC formed a 'Data Retention Project Team' involving the legal and compliance teams before significant changes to Chapter 4 came into effect in October 2015. The ACC engaged with our office, the Attorney-General's Department and other law enforcement agencies accessing telecommunications data; and the ACC's Acting Chief Executive Officer and representatives from its legal and compliance teams also attended 'metadata forums' hosted by our office. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
The ACC reported that it is compulsory for all staff members seeking access to prospective telecommunications data to receive training in the requirements of Chapter 4. The ACC also delivered compulsory tailored training sessions to authorised officers and has advised that it is developing compulsory training for staff seeking access to historic telecommunications data. In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks. For example, the Data Retention Project Team was appointed to produce recommendations directed at areas of compliance risk and these recommendations were tabled with an ACC executive committee. An

ACC executive committee also endorsed the creation of two additional full-time equivalent positions to work on the new requirements of Chapter 4, although these were not funded or appointed at the time of our inspection.

We noted effective communication and awareness-raising within the agency regarding compliance with Chapter 4. This included timely training, agency-wide emails and distribution of updated templates.

The ACC demonstrates a strong compliance culture. It encourages officers to report compliance issues, maintains a register of non-compliance and proactively discloses compliance issues to our office, which we commend.

4. Operation

The ACC's controls are not entirely automated and rely on the skills and experience of staff and embedded processes. For example: the compliance team performs quality assurance checks over prospective telecommunications data authorisations before they are provisioned; requests for historic telecommunications data are vetted by operational support staff before they are submitted to authorised officers (this quality assurance check is limited to one region at present, although the ACC advised that it would like to implement this process across all regional offices); and applicants must involve legal officers in the process if they identify that a JIW may be required.

The ACC has comprehensive standard operating procedures (SOPs) on accessing telecommunications data, which are updated as the need arises. These SOPs specifically address the requirements of Chapter 4 and are available to anyone seeking access to telecommunications data.

5. Performance Evaluation

We noted a number of compliance processes in place to self-evaluate the effectiveness of the ACC's compliance procedures. For example, in performing quality assurance checks over prospective data authorisations, the compliance team can identify any issues, and address these as part of its coordination and training role.

The compliance team also regularly reports to the ACC's audit committee on the agency's compliance with Chapter 4.

Australian Federal Police (AFP)

Stored communications inspection

We conducted our stored communications inspection of the AFP from 23 to 25 November 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Compliant, with the exceptions noted below and four instances where we were unable to determine compliance. We identified two instances where a stored communications warrant had been applied for and subsequently issued in respect of multiple persons, which is not provided for under the Act.[viii] We understand from the AFP's response that a contributing factor to this occurring was a lack of clarity in its warrant templates. Following a review by the TID, the AFP amended its templates in March 2016 to prevent further occurrences. We also identified six instances where warrants were exercised (served on the carrier) by a person not authorised under s 127(2).[xi] The AFP has since taken steps to address this issue. For three warrants, we were unable to determine whether certain stored communications had been sent by, or to, the person named on the warrant.[ix] As such, the AFP may have dealt with unlawfully accessed stored communications in contravention of s 133(1)(b)(ii) of the Act.[xii] To prevent any further contravention of the Act, we suggested that the AFP quarantine the stored communications until it can determine whether they were sent by, or intended for, the person named on the warrant. In one instance, we were unable to determine whether stored communications had been accessed by a carrier during the period the relevant warrant was in force.[x] In our view, the AFP should seek clarification from carriers when information as to the date and time of access is not provided. The AFP noted this finding, and advised that in future it will quarantine the relevant stored communications and contact the carrier for clarification. The AFP has procedures in place to monitor stored communications received, and quarantine those that have been unlawfully accessed. During the inspection, we noted instances where these procedures had worked well, which may indicate that the checks are being inconsistently applied. We suggest that the AFP may wish to review its procedures, particularly in relation to monitoring incoming product.

2. Has the agency properly managed accessed information?
Compliant, with one instance where we were unable to determine compliance. In this instance we were unable to determine who had received stored communications from a carrier in the first instance and, therefore, whether the communications had been properly received in accordance with s 135 of the Act.[xiii] Despite this instance, we noted that the AFP has effective procedures in place to record the particulars of the officer who received the stored communications.
3. Has the agency properly applied the preservation notice provisions?
Compliant, with one exception noted below and 25 instances where we were unable to determine compliance. The AFP self-disclosed one instance where a notice was revoked by an officer who was not authorised to do so under s 107M(2).[v] The AFP advised that this occurred as a result of the relevant officer using the incorrect revocation template. There were also three foreign preservation notices and 22 domestic preservation notices where we were unable to determine whether they should have been revoked in accordance with ss 107R(1) and 107L(2)(a)(ii) of the Act.[iv] We note the AFP's good practice of sending reminder emails to investigators at 30 day intervals during the period of effect of a preservation notice, to consider whether a notice should be revoked. However, it appears that investigators are not responding to these emails. We suggest that the AFP may wish to provide additional training for investigators on their legislative obligations under Chapter 3, and in particular, the requirement to revoke preservation notices in certain circumstances.
4. Has the agency satisfied certain record keeping and reporting obligations?
Compliant, noting that certain original records are located in the regions. This is consistent with our understanding of the AFP's procedures. We are of the view that the AFP has sufficient record keeping and reporting practices in place.
5. Was the agency cooperative and frank?
Compliant. The AFP has continued to be open and assistive during inspections. We commend the positive compliance culture promoted within the AFP, as demonstrated by its readiness to disclose any compliance issues to our office.

Telecommunications data inspection

We conducted our inspection of the AFP on 26 November 2016. Our findings against each inspection criterion are as follows.

1. Leadership
The AFP has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this was underpinned by the AFP executive's strong commitment to achieving compliance. For example, the Commissioner has requested to be briefed on every journalist information warrant (JIW) applied for by the AFP.
2. Planning
The AFP has plans in place to support compliance which include: comprehensive guidance materials on compliance with Chapter 4 within the "Investigator's Toolkit" available on the intranet; training packages which specifically address privacy concerns (a new requirement under Chapter 4); and templates for requesting access to telecommunications data with prompts to separate JIWs from standard authorisations. The AFP did not establish a formal metadata working group in the planning stage leading up to the new requirements of Chapter 4. One staff member took a major lead in preparing the agency for the significant changes to Chapter 4 in October 2015. This staff member is highly experienced, and has engaged with our office to inform the AFP's compliance framework. The AFP has contacted our office with queries regarding compliance with Chapter 4, and a Deputy Commissioner and those responsible for Chapter 4 compliance engaged in 'metadata forums' hosted by our Office. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
In addition to comprehensive training materials being available on the intranet to all staff seeking access to telecommunications data, the AFP also prepared tailored training materials for authorised officers which covers the new privacy and use and disclosure requirements under Chapter 4. This training package was delivered electronically to all authorised officers, however at the time of the inspection the AFP had no records of which authorised officers had reviewed the package. Moreover, we believe the training material for authorised officers could more specifically address compliance requirements for authorisations relating to foreign law enforcement agencies.

In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks. In addition to the strong support and involvement from its executive and its comprehensive internal guidance materials, the team responsible for managing telecommunications data requests are able to provide support to investigations staff.

We noted effective communication and awareness-raising within the agency regarding compliance with Chapter 4. For example, an agency-wide communiqué regarding the amendments to Chapter 4 was sent by a National Manager shortly before the changes to Chapter 4 took effect in October 2015. Targeted communiqués were also sent to authorised officers and investigators, and a 'metadata banner' was incorporated on the AFP's intranet hub page.

The AFP demonstrates a strong compliance culture. It encourages officers to report compliance issues, maintains a register of non-compliance and intend to proactively disclose compliance issues to our office which we commend.

4. Operation

Few of the AFP's controls for achieving compliance are automated and instead rely on the skills and experience of staff and embedded processes. For example, officers from the areas responsible for managing telecommunications data requests vet each authorisation, before a carrier is notified. The AFP's systems provide some automated controls, such as preventing requests exceeding legislated timeframes and not allowing content to be received inadvertently. The AFP also has processes in place to identify and quarantine any telecommunications data that may have been unlawfully obtained.

The AFP has standard operating procedures (SOPs) on accessing telecommunications data, which are updated as the need arises. These policies specifically address the requirements of Chapter 4 and are available to anyone involved in the process of accessing telecommunications data.

5. Performance Evaluation

We noted a number of compliance processes that are in place to self-evaluate the effectiveness of the AFP's compliance procedures. For example, the area responsible for administering telecommunications data requests maintains a 'metadata self-disclosures' register. This is an effective mechanism in ensuring common issues are identified and processes are updated to prevent reoccurrence.

Remedial Action

The AFP has since advised that it will assess various options to audit the completion of mandatory online training by authorised officers.

Australian Securities and Investments Commission (ASIC)

Telecommunications data inspection

We conducted our inspection of ASIC on 10 December 2015. Our findings against each inspection criterion are as follows.

1. Leadership
ASIC has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this is underpinned by the ASIC executive's strong commitment to achieving compliance. For example, prior to applying for a journalist information warrant (JIW), requesting officers are required to obtain written approval from an ASIC Commissioner (there are four Commissioners within ASIC who report to the Chairman).
2. Planning
ASIC has plans in place to support compliance which include: electronic templates for requesting and authorising access to telecommunications data with in-built JIW prompts; automated controls to ensure that applicants and authorised officers sufficiently consider privacy (a new requirement under Chapter 4); and a process for capturing the use and disclosures of telecommunications data. ASIC did not establish a formal metadata working group in the planning stage leading up to the implementation of the legislative amendments; although informal meetings between legal and intelligence support areas led to the development of redrafted policies, procedures, templates and training programs to achieve compliance with the requirements of Chapter 4. ASIC has contacted our office and the Attorney-General's Department with queries regarding compliance with Chapter 4. Additionally, a representative from ASIC's legal team, as well as staff involved in exercising powers, engaged in 'metadata forums' hosted by our office. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
ASIC reported that it had conducted training presentations with relevant teams seeking access to telecommunications data in October and November 2015. Attendance at this training was recorded and followed up on. Whilst ASIC does not provide tailored training to authorised officers, the legal team is in regular contact with authorised officers regarding Chapter 4's requirements.

In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations and to conduct ongoing assessment of compliance risks. For example, the legal team had a high level of involvement in the development and communication of ASIC's compliance framework. The legal team also monitors changes to legislation that might affect ASIC's compliance with Chapter 4 and communicates with the Attorney-General's department about telecommunications data when required.

ASIC demonstrated effective communication and awareness-raising within the agency regarding compliance with the Act. For example, ASIC's legal team sent an email to affected teams just before significant changes to Chapter 4 came into effect in October 2015. This email detailed the new privacy considerations and the procedures for prospective authorisations and JIWs.

4. Operation

ASIC has robust controls in place to support compliance, which are mostly automated and also rely on the skills and experience of staff and embedded processes. For example, before requests for telecommunications data are submitted to an authorised officer, they must be certified by a senior lawyer within ASIC. Furthermore, the team responsible for administering telecommunications data authorisations will manually vet the information received from carriers to ensure that it is within the remit of the authorisation.

ASIC has standard operation procedures (SOPs) on accessing telecommunications data, which are updated as the need arises. These SOPs specifically address the requirements of Chapter 4 and are available to anyone seeking access to telecommunications data.

5. Performance Evaluation

We noted that there were a number of compliance processes in place to self-evaluate the effectiveness of ASIC's compliance procedures. For example, before provisioning a request on to a carrier, each authorisation goes through two levels of approval, prior to consideration by an authorised officer. During this process verbal discussions can be held between requesting, approving, certifying and authorised officers about the compliance requirements of telecommunications data requests. We are of the view that this is a strong performance evaluation and compliance mechanism within the overall ASIC compliance framework.

Crime and Corruption Commission Queensland (CCC Qld)

Stored communications inspection

We conducted our stored communications inspection of the CCC Qld on 27 July 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Not assessed at this inspection.[10]
2. Has the agency properly managed accessed information?
Compliant, except in two instances where stored communications records remained on the CCC Qld's computer storage drives two months after the relevant destructions were said to have taken place. These records had not been destroyed forthwith, as is required by s 150(1).[xiv] We suggested creating a log for each stored communications warrant file which contains details of each location where accessed stored communications are held, in order to assist with the identification of relevant records during the destruction process. In response to this issue, the CCC Qld advised that the records which remained on its system had been overlooked during the destruction process, but were subsequently destroyed on 25 November 2016. As a result of our finding, the CCC Qld conducted an internal audit of all warrant files where information obtained under stored communications warrants was recorded as having been destroyed during the same period. This audit identified that stored communication records in relation to another six warrants had not been destroyed as previously reported. The CCC Qld advised that it is now in the process of destroying these files, and will report on these activities as required under s 150(2) of the Act.[xiv] To prevent this from occurring in future, the CCC Qld advised that officers who deal with the destruction of stored communication records have been provided with specific training on the requirements of s 150(1). In addition, the CCC Qld has updated its work instructions to require that officers include the location of all stored communication copies in its 'Use and Communication' Register, prior to initiating a destruction. We commend the CCC Qld for its responsiveness to this issue.

[10] The CCC Qld advised that it had not been issued with any stored communications warrants during the inspection period.

However, it appeared that the CCC Qld's destructions policy does not prescribe that all working copies must be destroyed following the chief officer's authorisation under s 150(1). We suggested that the CCC Qld update its destruction policy to reflect the requirements of s 150(1) regarding copies.

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

Compliant, except in one instance where a notice was left to expire though the carrier had advised the CCC Qld that there were no stored communications to preserve. This was in breach of s 107L(2)(a)(i) by virtue of s 107J(1)(c).[iv]

In response to this issue, the CCC Qld advised that it has updated its procedures to require that preservation notices are revoked pursuant to s 107L of the Act where a carrier has advised there are no stored communications to preserve.

Despite this instance, we are of the view that the CCC Qld has sound procedures in place regarding preservation notices. In particular, we commend the CCC Qld's practice of sending out monthly reminder emails to analysts with preservation notices in force. This practice assists the CCC Qld to ensure that notices are revoked where there is no longer an intention to seek a stored communications (or telecommunications interception) warrant, as is required by 107L(2)(a)(ii).[iv]

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

Compliant.

We are of the view that the CCC Qld has sufficient record keeping and reporting practices in place.

5. Was the agency cooperative and frank?

Compliant. The CCC Qld has continued to be open and assistive during inspections.

We also appreciate the CCC Qld's assistance in arranging access to operational staff members during the inspection. These staff members provided us with further information regarding the policies and procedures the CCC Qld has in place for ensuring compliance with the Act.

Telecommunications data inspection

We conducted our inspection of the CCC Qld on 23 March 2016. Our findings against each inspection criterion are as follows.

1. Leadership
The CCC Qld has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this is underpinned by CCC Qld management's strong commitment to achieving compliance. This was demonstrated by communications from the managers to staff accessing telecommunications data, emphasising personal accountability when exercising the powers and highlighting the new requirements of Chapter 4. The communications inspected confirmed that the CCC Qld has an overall focus on complying with the requirements of Chapter 4, particularly the strengthened privacy provisions (a new requirement under Chapter 4).
2. Planning
The CCC Qld has plans in place to support compliance which include: training on accessing telecommunications data for all new and existing staff; updated templates for authorising access to telecommunications data; an automated date range calculator for prospective telecommunications data authorisations; and guidance documents attached to each authorisation to assist with addressing privacy considerations. The CCC Qld advised that specific work instructions and templates for applying for journalist information warrants (JIWs) were in the process of being finalised. We note that the training delivered by the CCC Qld includes a section on JIWs. The CCC Qld involved relevant areas in the planning stage (each team seeking to access telecommunications data, legal, IT, governance) in an informal working group. CCC Qld staff involved in exercising powers and those responsible for Chapter 4 compliance have engaged in 'metadata forums' hosted by our office; however none of the CCC Qld executive attended our office's heads-of-agency 'metadata forum'. The CCC Qld also invited us to discuss the initial development of its compliance framework, prior to significant changes to Chapter 4 coming into effect in October 2015. We feel that this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
The CCC Qld reported that it is compulsory for all staff who access telecommunications data to receive training in the requirements of Chapter 4, however it does not provide role specific training for authorised officers. Individual work instructions and an authorised officer checklist are available, and provide

information about the role of an authorised officer, with specific guidance on Chapter 4's requirements.

In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks. Due to the size of the CCC Qld, it has a small cohort of experienced staff. For example, in practice most requests for telecommunications data at the CCC Qld are approved by a single authorised officer who is very experienced. This authorised officer sits on the CCC Qld's operational committees and so has a general understanding of the investigations which are in progress.

We noted effective awareness-raising within the agency regarding compliance with Chapter 4. Regular communications from management informed staff of common compliance issues and helped to maintain a high level of awareness about the requirements of Chapter 4.

4. Operation

The CCC Qld has controls in place to support compliance; these are not completely automated but largely reliant on the skills and experience of staff as well as processes. There are multiple levels of quality assurance, including additional involvement from the recommending officer in each authorisation, and guidance documents attached to each authorisation which assists staff in achieving compliance with the requirements of Chapter 4.

The CCC Qld has standard operating procedures (SOPs) on accessing telecommunications data, which are updated as the need arises. These SOPs specifically address the requirements of Chapter 4, except for those around JIWs, and are available to all staff involved in the application process for metadata.

5. Performance Evaluation

We noted at inspection that the CCC Qld has formal processes in place to self-evaluate the effectiveness of its compliance procedures. For example, the CCC Qld keeps records on applications rejected by authorised officers, including notes in its records management system as to why these applications were rejected. We are of the view that this practice will allow the CCC Qld to efficiently target future training programs for staff on compliance with Chapter 4.

Remedial Action

The CCC Qld has advised that, subsequent to the inspection, a set of work instructions and associated templates for JIWs had been completed and made available to CCC Qld officers. Furthermore, these work instructions are included in the CCC Qld's online training programs which are available to all officers who deal with telecommunications data.

Department of Immigration and Border Protection (DIBP)

Stored communications inspection

We conducted our stored communications inspection of the Australian Customs and Border Protection Service (Customs)[11] on 18 February 2016. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Unable to determine compliance. No stored communications product was made available for our inspection. Therefore, we cannot provide assurance that Customs was only dealing with lawfully accessed information, as required by s 133(1)(b)(ii) of the Act.[xii] Furthermore, in five instances we were unable to determine whether carriers had accessed stored communications during the period that the relevant warrant was in force.[x] In these instances, no records (generally a coversheet completed by the carrier) were available which indicated the date and time of carrier access. When this information is not apparent, Customs should seek clarification from carriers. Customs should also quarantine the stored communications until such clarification is received to prevent any dealing with stored communications in contravention of s 133(1)(b)(ii) of the Act. In our view, Customs does not have sufficient processes in place to demonstrate that it is only dealing with lawfully accessed stored communications. **Recommendation 1:** That the Australian Customs and Border Protection Service implement processes to demonstrate that it is only dealing with stored communications that have been lawfully accessed.
2. Has the agency properly managed accessed information?
Unable to determine compliance.

[11] The operational and enforcement functions of Customs are now carried out by the Australian Border Force within the DIBP, which was established on 1 July 2015. We note, however, that the records inspected were created while the Customs was still an entity. As such, we have continued to refer to Customs for the purpose of our inspection findings.

In every instance, we were unable to determine who had received the stored communications from the carrier and, therefore, whether the communications had been properly received in accordance with s 135 of the Act.[xiii]

Furthermore, for the assessed destruction of stored communications, there were no records available to demonstrate who within Customs had authorised the destruction to occur or when the approval had been granted. As a result, we could not determine whether it was done in accordance with s 150(1) of the Act.[xiv]

In our view, Customs does not have sufficient procedures in place to ensure that stored communications are properly received and destroyed.

Recommendation 2:

That the Australian Customs and Border Protection Service implement processes to demonstrate that accessed stored communications have been managed in accordance with ss 135 and 150(1).

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

Non-compliant.

Eleven of the 14 historic preservation notices which fell within the inspection period were given in breach of s 107M(1) of the Act.[v] In these instances, the officers who gave the notices had not been nominated by the chief officer under s 110(3) of the Act, and were therefore not authorised to apply for stored communications warrants (or give domestic preservation notices) on behalf of Customs.[vii]

We note that Customs updated its nomination under s 110(3) at the end of the inspection period, therefore no recommendation has been made.

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

Non-compliant.

We cannot provide assurance that Customs has kept each preservation notice given and warrant issued, as is required by ss 150A(a) and 151(a) of the Act.[xv]

Prior to the inspection, Customs advised our office that it had given 14 preservation notices and been issued with 10 stored communications warrants during the inspection period, and provided us with a list of the same.

At the inspection, we identified the following issues:

- Three of the preservation notices from Customs' list could not be located.

- The reference number used for one of the missing preservation notices had also been used to identify another preservation notice given ten days earlier. The second preservation notice was also missing.
- Three additional preservation notices were found which had not been included in Customs' list, though each fell within the inspection period.
- Two additional warrants were found which had not been included in Customs' list, although both fell within the inspection period.
- There was evidence to suggest that Customs had been issued with another stored communications warrant during the inspection period which it had also failed to include in its list. This warrant was not provided to us.

A contributing factor to these issues is Customs' unreliable referencing system for preservation notices and warrants:

- The references used do not appear to be sequential, nor do they clearly identify the financial year to which the record relates.
- Some preservation notices follow a different system entirely – these are identified by task numbers.
- The same reference number is used to identify multiple warrants and preservation notices. At this inspection, this led to five instances where Customs failed to advise our office of the existence of stored communications warrants and preservation notices.

We have no confidence in Customs' record keeping practices, and therefore in its ability to account for its use of these powers.

The following recommendation is again made:

Recommendation 3:

That the Australian Customs and Border Protection Service implement a new record keeping and referencing system for its stored communications warrants and preservation notices.

5. Was the agency cooperative and frank?

Non-compliant with the exception of staff from one branch, who were cooperative and attempted to provide our office with access to relevant information. However, the inspection was not well coordinated or prepared for.

Customs' response and advised actions

In response to the draft report, Customs acknowledged the record-keeping shortfalls identified at the inspection. Customs indicated that the period to which the report relates (1 July 2014 to 30 June 2015) was a time of significant organisational

disruption as it moved towards integration with the Department of Immigration and Border Protection.

Customs advised that urgent action has commenced to ensure that robust and transparent arrangements are in place to satisfy its reporting obligations, and provide a framework for lawfully accessing, managing and preserving stored communications under the Act.

As advised by Customs, the steps taken include:

- Developing procedural instructions and a detailed standard operating procedure to provide clear guidance on record keeping requirements and managing stored communications in accordance with the Act.
- Developing a record keeping system for all stored communications warrants and preservation notices.
- Establishing a central point of contact for all departmental requests relating to the application for and destruction of stored communications.

Customs expects these actions to be substantially implemented by 1 July 2017. In addition, Customs advised that it intends to monitor and track the implementation of the report's recommendations, including via an internal audit conducted as part of its 2017-18 strategic assurance program.

Customs also noted the report's finding that the inspection was not well coordinated or prepared for. Customs advised that an internal investigation into the matter had shown this deficiency to have been the result of the absence of a central coordinating point for the inspection. In response to this finding, Customs has established a central point of coordination in its Audit and Assurance Branch to coordinate preparations for our inspections.

Customs has acknowledged that access to stored communications is a significant power, and noted the seriousness with which it regards its responsibilities under Chapter 3 of the Act. We will assess the effectiveness of its remedial actions at future inspections.

Telecommunications data inspection

We conducted three inspection visits of the DIBP in Canberra on 17 November 2015, Sydney on 2 December 2016 and Adelaide on 12 May 2016. Our findings against each inspection criterion are as follows.

1. Leadership
The DIBP did not demonstrate that it has clear organisational roles and responsibilities in place to support compliance within its senior levels. During the inspection, it was clear that a high level of personal accountability exists at operational levels of the agency, which is underpinned by a strong quality assurance process. It is our view that executive and senior management support for the activities occurring at the operation level would help promote continual improvement and foster the development of a strong compliance culture at the agency. The DIBP has since advised our office that the senior executive has been actively supporting operational staff in developing a robust Chapter 4 continual improvement and compliance culture. This has been demonstrated by the senior executive receiving weekly briefings on the operations and workload of the telecommunications team; briefings which contain issues relevant to the DIBP's compliance with Chapter 4.
2. Planning
The DIBP has plans in place to support compliance which include: a detailed standard operating procedure (SOP) manual which explains the legislative and policy background of telecommunications data requests and outlines how to make requests for telecommunications data; templates for making requests; monthly newsletters; telecommunications data 'cheat sheets'; and training. The DIBP has contacted our office on a number of occasions with queries about compliance with Chapter 4. Additionally, members of the DIBP's operational and compliance staff engaged in a 'metadata forum' hosted by our office. We feel this demonstrates planning and preparedness for demonstrating compliance with Chapter 4 by operational staff; however no member of the DIBP's executive attended a heads-of-agency 'metadata forum' hosted by our office, which we feel further demonstrates a lack of involvement by the DIPB executive in developing a Chapter 4 compliance framework.
3. Support
The DIBP advised that staff processing telecommunications data requests are required to undertake mandatory training prior to making requests. This training includes topics such as culture and conduct, disclosure of official information, risk management, security and privacy. Staff are also encouraged to undertake training on the various DIBP's systems, intelligence collection, research, and an overview of the telecommunications industry. Additionally, authorised officers are

provided with an authorised officer guide, which has guidance on their specific responsibilities.

It was noted at inspection that, while the authorised officer role at the DIBP is delegated to senior executive officers, in practice the authorised officer delegation is exercised predominately at a non-executive level.

At the inspection our office was advised that key officers involved in implementing the data retention amendments were no longer engaged in compliance roles at the agency. Although there is a risk that corporate knowledge may be lost with the movement of key staff, this risk is somewhat mitigated by detailed SOPs and telecommunications data checklists.

The DIBP demonstrated effective communication and awareness-raising within the agency regarding compliance with the Act. The team which authorises and processes authorisations has played an important role in communicating information on compliance to the wider agency. This has been achieved via monthly newsletters, quarterly videoconferences with regional officers, procedural updates, and the use of a group email for receiving telecommunications data requests and queries.

4. Operation

The DIBP has some automated controls, such as the auditability of its 'Request for Information' system, but for the most part the agency is heavily reliant on the skills and experience of staff and a multi-level quality assurance process. The DIBP's telecommunications data application templates specifically address the requirements of Chapter 4 of the Act, which are then reviewed at each stage of the quality assurance and authorisation process.

While the SOPs on accessing telecommunications data are comprehensive in other aspects of Chapter 4's requirements, at the time of inspection, there was limited guidance on applying for journalist information warrants.

5. Performance Evaluation

Based on advice from the DIBP and our observations, the DIBP has formal and informal processes in place to self-evaluate the effectiveness of its compliance procedures. For example, requests must first go through an information officer as part of the quality assurance process. In addition to this, each time an authorisation is returned to a requesting officer for amendment by an authorised officer, a copy of and reason for return is retained.

It is our view that the DIBP could improve its performance evaluation processes by conducting internal audits of its compliance procedures to identify areas of risk and implement controls to mitigate these risks.

Remedial Action

The DIBP has advised that it agrees clear senior executive accountability and governance is critical to the support and development of a Chapter 4 compliance framework. The DIBP informed our office that, subsequent to our inspection, a Deputy Secretary visited the telecommunications team and obtained a thorough face to face briefing on the process for authorising requests for information under Chapter 4. In addition, the Deputy Secretary observed a demonstration of the system used to process, log and audit requests for information under Chapter 4.

The DIBP also advised that it has updated the SOPs to implement an additional control mechanism for certain categories of authorisations, whereby the request for telecommunications data must be forwarded to its legal area for advice before proceeding.

Finally, the DIBP agreed that, resources and priorities permitting, internal audits would further strengthen its existing processes.

Independent Broad-based Anti-Corruption Commission (IBAC)

Telecommunications data inspection

We conducted our inspection of the IBAC on 3 May 2016. Our findings against each inspection criterion are as follows.

1. Leadership
IBAC has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this is underpinned by IBAC executive's strong commitment to achieving compliance. This was demonstrated by the executive resourcing IBAC's purpose-built database, through which all telecommunications data authorisations are applied for, approved and retained.
2. Planning
IBAC has plans in place to support compliance which include: training in the requirements of Chapter 4; automated controls to ensure that applicants include sufficient information to address privacy concerns (a new requirement under Chapter 4); and a process for capturing the use and disclosure of telecommunications data. IBAC involved all relevant areas in the planning stage (each team seeking access to telecommunications data, information technology and the legal and compliance team) in a formal 'metadata' working group. IBAC has contacted our office with queries regarding compliance with Chapter 4, and the Chief Executive Officer and those responsible for Chapter 4 compliance engaged in 'metadata forums' hosted by our Office. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
IBAC reported that it is compulsory for all staff members seeking access to telecommunications data to receive training in the requirements of Chapter 4. IBAC also provided tailored training to authorised officers and affected operational staff before significant changes to Chapter 4 came into effect in October 2015. In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks. In addition to the strong support and involvement from its executive, IBAC's combined legal and compliance team set up its purpose-built database with input from IBAC's operational and technical teams.

Access to the database is managed by the legal and compliance team, who also provide support to operational officers in their use of the database.

We noted effective communication and awareness-raising within the agency regarding compliance with Chapter 4. This included timely training, an agency-wide information session, an intranet announcement and an email to operational staff.

4. Operation

IBAC has robust controls to support compliance which are automated by its purpose built database. IBAC also draws upon the skills and experience of its staff, for example, legal and compliance officers support applicants through the Journalist Information Warrant (JIW) process and all JIW applications are subject to review by the Managing Lawyer or General Counsel.

IBAC has comprehensive standard operating procedures (SOPs) on accessing telecommunications data, which are updated as the need arises. These SOPs specifically address the requirements of Chapter 4 and are available to anyone seeking access to telecommunications data.

5. Performance Evaluation

We noted that there were a number of processes in place to self-evaluate the effectiveness of IBAC's compliance procedures. For example, the purpose built database has a function that allows authorised officers to return requests to the applicant for further work and captures this feedback in the system. There is also a requirement (reinforced in the SOPs and training sessions) for officers to notify the legal and compliance team if any content is provided by a carrier. The legal and compliance team is well placed to use this information to identify and address issues as part of its coordination and training role.

Independent Commission Against Corruption New South Wales (ICAC NSW)

Stored communications inspection

We conducted our stored communications inspection of the ICAC NSW on 2 September 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Not assessed at this inspection.[12]
2. Has the agency properly managed accessed information?
Compliant, with the exception of ICAC NSW's advised practice of destroying working copies without the chief officer's approval. The ICAC NSW advised that it routinely deletes working copies of stored communications due to storage space limitations on the system used to receive the communications from this carrier. We suggested that the chief officer be made aware of this practice, as they are ultimately responsible for the ICAC NSW's destruction obligations under s 150(1).[xiv] In response to this finding, the ICAC NSW advised that the relevant system has been decommissioned by the carrier. While this may resolve the issue for future records, we suggest that the ICAC NSW keep our suggestion in mind for any replacement system. Overall, we note the good practices that the ICAC NSW has in place for keeping track of all stored communications, being definitive about the location where accessed information is held and keeping particulars regarding each destruction.
3. Has the agency properly applied the preservation notice provisions?
Compliant. We are of the view that the ICAC NSW has sufficient procedures in place regarding preservation notices.
4. Has the agency satisfied certain record keeping and reporting obligations?
Compliant.

[12] The ICAC NSW advised that it had not been issued with any stored communications warrants during the inspection period.

We are of the view that the ICAC NSW has sufficient record keeping and reporting practices in place.

5. Was the agency cooperative and frank?

Compliant. The ICAC NSW has continued to be open and assistive during inspections.

We also appreciate the ICAC NSW's assistance in arranging for access to operational staff members during the inspection. These staff members provided us with further information regarding the policies and procedures the ICAC NSW has in place for ensuring compliance with the Act.

Telecommunications data inspection

We conducted our inspection of the ICAC NSW on 9 December 2015. Our findings against each inspection criterion are as follows.

1. Leadership
The ICAC NSW has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this was underpinned by strong commitment from the ICAC NSW's executive, as demonstrated by its involvement in determining policies and procedures prior to significant changes to Chapter 4 coming into effect in October 2015, as well as their continued monitoring of compliance outcomes for the agency.
2. Planning
The ICAC NSW has plans in place to support compliance which include: training for all investigations staff and authorised officers in the requirements of Chapter 4; an onus on those applying for access to telecommunications data to sufficiently address privacy (a new requirement under Chapter 4); and specific training and guidance material regarding journalist information warrants. The ICAC NSW involved all relevant areas in the planning stage (the executive, investigations, specialised compliance and legal areas), with all associated policy and procedures requiring approval by the Executive Committee. The ICAC NSW engaged with other agencies accessing telecommunications data regarding compliance with Chapter 4, and the ICAC NSW executive and staff engaged in 'metadata forums' hosted by our office. We feel that this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
It appeared that the ICAC NSW delivered training to all its investigators in the requirements of Chapter 4. The ICAC NSW also advised that a more detailed version of the training session was delivered to authorised officers and most of its legal staff. In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks. In addition to the strong support and involvement from its executive, internal guidance materials are comprehensive; and the specialised compliance area is enabled to provide support to investigations staff. We noted effective internal communications and awareness-raising within the agency regarding compliance with Chapter 4. This included various channels

through which risks to compliance with Chapter 4 may be noted, identified and acted upon throughout the ICAC NSW.

The ICAC NSW demonstrates a strong compliance culture.

4. Operation

The ICAC NSW has strong controls in place to support compliance. These are not automated but heavily reliant on the skills and experience of staff as well as embedded processes. This includes templates which prompt both the applicant and authorised officer to have the necessary considerations as well as vetting procedures by the ICAC NSW's specialised compliance area.

The ICAC NSW has a comprehensive operations manual relating to telecommunications data which is updated as the need arises. The operations manual specifically addresses the requirements of Chapter 4 and is available to anyone involved in the process of accessing telecommunications data.

5. Performance Evaluation

We noted that there were a number of compliance processes in place to self-evaluate the effectiveness of the ICAC NSW's compliance procedures. These processes include the ability to identify issues during vetting procedures and effective internal communication forums, including monitoring of compliance outcomes by the ICAC NSW executive.

Independent Commissioner Against Corruption South Australia (ICAC SA)

Telecommunications data inspection

We conducted our inspection of the ICAC SA on 11 May 2016. Our findings against each inspection criterion are as follows.

1. Leadership
The ICAC SA has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this was underpinned by senior management and the executive's commitment to implementing an effective compliance framework, as demonstrated by the attendance of both at training sessions covering the new requirements of Chapter 4. In addition, delegations for authorised officers are restricted to the executive and one senior manager. In our view the direct involvement of the ICAC SA executive in the authorisation process acts as an effective control within ICAC SA's compliance framework.
2. Planning
The ICAC SA has plans in place to support compliance which include: an onus on those applying for access to telecommunications data to sufficiently address privacy (a new requirement under Chapter 4); and a process to identify any circumstances where a journalist information warrant (JIW) may be needed. We noted that the ICAC SA's telecommunications data policy does not provide specific detail on the role and responsibilities of authorised officers under Chapter 4, although this information was covered during training presentations given to investigators and legal officers. While there are three authorised officers at the ICAC SA, in practice most requests are approved by a single authorised officer who is highly experienced. To address the continuity risk, however, we suggest that a section on the responsibilities of authorised officers is included in the ICAC SA telecommunications data policy. The ICAC SA formed an informal telecommunications data working group comprising relevant areas in the compliance planning stage, including investigators, intelligence analysts, legal officers and senior executive officers. Furthermore, the ICAC SA's primary authorised officer meets fortnightly with its investigation team and forensic officers to discuss ongoing work and changes that will impact the agency, which, when required, involves a discussion of telecommunications data. The ICAC SA has engaged with other agencies accessing telecommunications data in preparing for its obligations under Chapter 4, and ICAC SA compliance staff engaged in 'metadata forums' hosted by our office, although none of the

ICAC SA executive attended our office's heads-of-agency 'metadata forum'. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.

3. Support

The ICAC SA reported that compliance training is compulsory for all staff members involved in accessing telecommunications data. In addition, the ICAC SA provided specific training to legal officers which covered JIWs in detail. All training was attended by the ICAC SA executive.

In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks. The ICAC SA's legal team has been involved in planning for and establishing JIW processes. The structure of the ICAC SA allows for compliance support to be provided to investigators by intelligence analysts and the ICAC SA's telecommunications compliance officer.

We noted effective communication and awareness-raising within the agency regarding compliance with Chapter 4. This included timely training on the requirements of Chapter 4 and the development and distribution of standard operating procedures (SOPs).

The ICAC SA demonstrates a strong compliance culture.

4. Operation

The ICAC SA's compliance controls are not completely automated and rely on the skills and experience of staff and embedded processes. For example, intelligence analysts check applications for compliance with the requirements of Chapter 4 and the legal team are engaged if a JIW may be required.

The ICAC SA has comprehensive SOPs on accessing telecommunications data, which are updated as the need arises. These SOPs specifically address the requirements of Chapter 4 and are available to anyone involved in the process of accessing telecommunications data. The SOPs were distributed to relevant staff by the telecommunications compliance officer immediately after significant changes to Chapter 4 came into effect in October 2015.

5. Performance Evaluation

We noted that there were a number of compliance processes in place to self-evaluate the effectiveness of the ICAC SA's compliance procedures. For example, the telecommunications compliance officer and legal team address any issues as part of their coordination and training role. Informal discussions are also held between requesting officers and authorising officers about applications, which serve to self-evaluate the effectiveness of processes. The ICAC SA advised that intelligence analysts perform quality assurance checks on all telecommunications

data received from carriers, prior to that information being accessed by investigators. We are of the view that this acts both as an effective control and a performance evaluation measure within the overall ICAC SA compliance framework.

Remedial Action

The ICAC SA advised that it has reviewed and amended its data policy to specifically outline the responsibilities of authorised officers when considering whether to issue a data authorisation. The data policy was also updated to reflect structural changes within the ICAC SA's investigations team.

New South Wales Crime Commission (NSWCC)

Stored communications inspection

We conducted our stored communications inspection of the NSWCC on 1 September 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Compliant, except in one instance. A stored communications warrant authorises access, subject to any conditions or restrictions, to stored communications: • made by the person in respect of whom the warrant was issued, or • that another person has made, where the intended recipient is the person in respect of whom the warrant was issued.[ix] In this instance, we were unable to establish a link between the person named on the warrant and some of the stored communications accessed. Two of the three telecommunications services accessed under the warrant did not appear to have been used by the targeted person. We suggest that the NSWCC quarantine from further use any stored communications which were not made by, or intended for, the person named on the warrant. The NSWCC has a monitoring checklist in place for ensuring that it only deals with lawfully accessed stored communications. While we commend the NSWCC for implementing this procedure, we believe that it could be strengthened by including checks for whether all stored communications relate to the person in respect of whom the warrant was issued, and whether any warrant restrictions or conditions were adhered to.
2. Has the agency properly managed accessed information?
Compliant. Nothing came to our attention to suggest that the NSWCC had not properly managed accessed information. We are of the view that the NSWCC has sound procedures in place for managing information accessed under a stored communications warrant. In particular, we commend the NSWCC's use of a log on each warrant file to record the number of copies of accessed stored communications that have been made, and where each

copy is located. This practice assists the NSWCC in accounting for all copies of stored communications which assists compliance with its destruction obligations.
3. Has the agency properly applied the preservation notice provisions?
Compliant, with one instance where we were unable to determine compliance with mandatory revocation requirements under s 107L(2)(a)(ii) of the Act.[iv] Despite this instance, we are of the view that the NSWCC has sufficient procedures in place regarding preservation notices.
4. Has the agency satisfied certain record keeping and reporting obligations?
Compliant. We are of the view that the NSWCC has sufficient record keeping and reporting practices in place.
5. Was the agency cooperative and frank?
Compliant. The NSWCC has continued to be open and assistive during inspections.

Telecommunications data inspection

We conducted our inspection of the NSWCC on 1 December 2015. Our findings against each inspection criterion are as follows.

1. Leadership
The NSWCC has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was noted that the NSWCC executive has a strong commitment to implementing an effective Chapter 4 compliance framework. This was demonstrated by the Commissioner and senior executives opening and attending metadata training seminars, which outlined changes to Chapter 4 and highlighted the need for personal accountability at the agency. These seminars also allowed the executive to report to staff on their attendance at the heads of agencies meeting facilitated by our office, which discussed the requirements of Chapter 4. We also note that some of the NSWCC executive are present at fortnightly analyst meetings, which involve discussions of telecommunications data.
2. Planning
The NSWCC has plans in place to support compliance which include: compulsory training in the requirements of Chapter 4 for authorised officers; an onus on requesting officers to provide sufficient information in applications; and a process to identify any circumstances where a journalist information warrant (JIW) may be needed. The NSWCC formed a 'metadata' working group comprising relevant areas in the compliance planning stage including senior executives working with legal, governance, records management and investigation teams. The NSWCC executive is also responsible for consideration and final approval of all updated agency policies and procedures, including the comprehensive and recently updated 'Chapter 4 compliance policy'. The NSWCC has contacted our office with queries about compliance with Chapter 4. The Commissioner, senior executive officers, and staff involved in exercising powers and compliance have also engaged in 'metadata forums' hosted by our office. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4's requirements.
3. Support
The NSWCC reported that it is compulsory for authorised officers to receive targeted training in the requirements of Chapter 4. In addition, two training seminars were held for investigators who are involved in accessing telecommunications data, as well as legal staff and governance officers.

In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks. The executive's support for and involvement in developing an effective compliance framework is high. The NSWCC's governance and legal units have each been involved in planning as well as establishing processes for applying for JIWs. The warrant administration team is able to provide relevant support to investigations staff when required.

We noted effective communication and compliance awareness-raising within the agency regarding compliance with Chapter 4. This included updating and distributing standard operating procedures (SOPs), all staff emails reminding staff of compliance requirements under Chapter 4, and training seminars backed by executive support.

The NSWCC demonstrates a strong compliance culture.

4. Operation

The NSWCC's compliance controls are not completely automated and rely on the skills and experience of staff and embedded processes. Although not automated, the warrant administration team check applications for compliance with Chapter 4 of the Act and the legal unit are engaged if a JIW is required.

The NSWCC has comprehensive SOPs on accessing telecommunications data, which are updated as the need arises. These SOPs specifically address the requirements of Chapter 4 and are available to anyone involved in the process of accessing telecommunications data. The updated SOPs were distributed to relevant staff by the governance unit after significant changes to Chapter 4 came into effect in October 2015.

5. Performance Evaluation

We noted that there were a number of compliance processes in place to self-evaluate the effectiveness of the NSWCC's compliance procedures. For example, the warrant administration team and governance unit address gaps in processes as part of their coordination role and informal discussions between requesting officers and authorised officers serve to self-evaluate the effectiveness of processes.

In addition to the Ombudsman's inspection, the NSWCC's internal auditor oversees agency compliance with the requirements of Chapter 4, which should assist the NSWCC to achieve compliance with Chapter 4 of the Act.

On 27 June 2016 our office received a report from the NSWCC which detailed the results of the first internal audit of telecommunications data requests under Chapter 4. This indicated that there was a high level of compliance with the new authorisation requirements under Chapter 4 and that the NSWCC maintained sufficient records to meet the new record keepings provisions under Chapter 4 of

the Act. The report also indicated that the NSWCC has effective and working processes to manage inadvertent disclosures from carriers.

New South Wales Police Force (NSWPF)

Stored communications inspection

We conducted our stored communications inspection of the NSWPF from 10 to 13 August 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Compliant. Nothing came to our attention to suggest that the NSWPF had dealt with unlawfully accessed stored communications. We are of the view that the NSWPF has effective screening and quarantining procedures in place to ensure that it is only dealing with lawfully accessed stored communications. This was demonstrated in two instances where carriers provided the NSWPF with stored communications for a service not authorised by the warrant, or had been accessed after the warrant had expired. In each instance, the NSWPF identified the carrier's error immediately after receiving the product and took appropriate remedial actions – quarantining the product and seeking legal advice where appropriate.
2. Has the agency properly managed accessed information?
Compliant, with the exception of eight instances where stored communications records were not destroyed in accordance with s 150(1) of the Act. Under s 150(1) of the Act, if the chief officer of the agency is satisfied that a record obtained by accessing stored communications is not likely to be required, then the chief officer must cause the record to be destroyed forthwith.[xvi] In these instances, we located stored communications discs in the archives room for warrants which had been certified for destruction by the chief officer. This appears to have occurred as the result of investigators returning discs after the relevant destruction round has been carried out. We are of the view that the NSWPF's procedures regarding destructions could be strengthened through the inclusion of a reconciliation of stored communications discs. To facilitate this, we suggested that the NSWPF may wish to give the officer primarily responsible for destructions access to its evidence management database, if it has not done so already. The NSWPF has acknowledged the deficiency with its previous destruction system and advised that its systems have since been updated to address the issue.

3. Has the agency properly applied the preservation notice provisions?
Compliant, with the exception of one instance self-disclosed by the NSWPF where a carrier preserved stored communications for a person other than the subject of the preservation notice, contrary to s 107H(1).[i] This occurred due to a typographical error in the electronic request to the carrier accompanying the preservation notice. The carrier identified the error on receiving the warrant and no preserved product was provided to the NSWPF. The NSWPF advised that it has amended its practices to reduce the likelihood of this occurring in future. Despite this instance, we are of the view that the NSWPF has sufficient procedures in place regarding preservation notices.
4. Has the agency satisfied certain record keeping and reporting obligations?
Compliant. The NSWPF implemented individual referencing systems for preservation notices and stored communications warrants in March 2014. Based on the records made available for inspection, it appears that these referencing systems are effective at ensuring compliance with the Act.
5. Was the agency cooperative and frank?
Compliant. The NSWPF has continued to be open and assistive during inspections. We appreciate the NSWPF's assistance in arranging for access to operational staff members during the inspection, who provided us with further information regarding the policies and procedures the NSWPF has in place for ensuring compliance with the Act. Above all, we would like to commend the positive compliance culture promoted by the NSWPF, as demonstrated by its readiness to disclose any compliance issues to our office. The NSWPF also facilitates workshops and meetings with our office to ensure that it remains vigilant to emerging issues and best practice.

Telecommunications data inspection

We conducted our inspection of the NSWPF on 7 December 2015. Our findings against each inspection criterion are as follows.

1. Leadership
The NSWPF has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this is underpinned by the executive's strong commitment to achieving compliance, as demonstrated by the attendance of the Commissioner for the NSWPF at a 'metadata forum' hosted by our office. The NSWPF also initiated its own 'metadata forum' to discuss pertinent issues, inviting our office and the Attorney-General's Department to attend together with other NSW law enforcement agencies. We note the NSWPF's openness to share knowledge of their compliance systems, in the spirit of cooperation, with other agencies.
2. Planning
The NSWPF has plans in place to support compliance which include: frequent engagement with our office outside the inspection process; implementing enhancements to systems to ensure compliance with Chapter 4 can be achieved and demonstrated; and embedding processes to ensure that privacy concerns are considered (a new requirement under Chapter 4) and the need for journalist information warrants (JIW) are identified. The NSWPF involved relevant areas in the planning stage (compliance, operations, specialist support and corporate services) as part of a formal 'data retention implementation working group'. The NSWPF has shown strong representation at the recurring 'metadata committee' meetings convened by the Attorney-General's Department. The NSWPF has also frequently contacted our office with requests for advice regarding compliance thresholds. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
The NSWPF has made training available to all staff members involved in accessing telecommunications data, including authorised officers. The head of the telecommunications compliance area produced an agency-wide training and awareness video on the intranet. Training was also complemented by prompts on relevant systems and forms, and the requirement to pass a monthly quiz in order to access the system for prospective telecommunications data.

In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks. Additionally, operational support for achieving compliance is high, for example, the NSWPF's legal team has been involved in the JIW process and is available 24 hours a day to provide advice to officers. There is also an in-house service centre which provides support for the NSWPF's purpose-built system (primarily used to apply for, approve and provision historic telecommunications data authorisations).

We noted effective communication and awareness-raising within the NSWPF regarding compliance with Chapter 4. This included intranet announcements, updates in a monthly newsletter and 'metadata screen savers' on agency computers.

The NSWPF demonstrates a strong compliance culture supported by a high level of personal accountability, especially from the authorised officers.

4. Operation

The NSWPF has strong controls in place to support compliance which are mostly automated and are supported by the skills and experience of staff and embedded processes. For example, applicants must involve the legal team and the telecommunications compliance area if they identify that a JIW may be required.

The NSWPF has comprehensive standard operating procedures (SOPs) on accessing telecommunications data, which are updated as the need arises. The SOPs specifically address the requirements of Chapter 4 and are available to anyone seeking access to telecommunications data.

5. Performance Evaluation

We noted that there were a number of compliance processes in place to self-evaluate the effectiveness of the NSWPF's compliance procedures. For example, its purpose-built system enables an authorised officer to provide feedback when rejecting a historic telecommunications data request by recording the reasons in a free-text box. In addition, the telecommunications compliance area advised that it keeps records of each rejection of a prospective telecommunications data request. The telecommunications compliance area is well placed to use this information to identify and address issues as part of its coordination and training role.

Northern Territory Police

Stored communications inspection

We conducted our stored communications inspection of the Northern Territory Police on 16 and 17 May 2016. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Compliant, though in four instances we were unable to determine whether the Northern Territory Police had only dealt with lawfully accessed information, as required by s 133(1)(b)(ii).[xii] This occurred because the carrier provided the stored communications on password protected discs, and the Northern Territory Police advised that it had misplaced the passwords. In order to demonstrate compliance with this criterion, we suggested that the Northern Territory Police implement a consistent process for storing carrier passwords, whereby passwords are kept in hardcopy on the relevant warrant files, or in softcopy in an electronic register.
2. Has the agency properly managed accessed information?
Compliant. Nothing came to our attention to indicate that the Northern Territory Police had not properly managed accessed information during this inspection period; however, we note that the Northern Territory Police has not yet complied with the Act's requirements in relation to records from previous inspection periods.
3. Has the agency properly applied the preservation notice provisions?
Compliant. We are of the view that the Northern Territory Police has sufficient procedures in place regarding preservation notices.
4. Has the agency satisfied certain record keeping and reporting obligations?
Compliant, though we were unable to determine whether each evidentiary certificate issued by the Northern Territory Police under s 130(1) had been kept, as is required by s 151(c) of the Act.[xv] At the inspection we were not presented with any evidentiary certificates, however one team advised that it prepares the evidentiary certificates for the Northern Territory Police. After the certificate is signed by a certifying officer, this team provides the original to the investigator, and no copy is kept centrally.

In order to demonstrate compliance, we suggested that this team retain a copy of each evidentiary certificate issued for inspection purposes.
5. Was the agency cooperative and frank?
Compliant. The Northern Territory Police has continued to be open and assistive during inspections. The Northern Territory Police was also very receptive to our best practice suggestions made at the inspection.

Northern Territory Police's response and advised actions

In response, the Northern Territory Police advised that the suggestions in our draft report have now been put into place and will assist the Northern Territory Police to better demonstrate compliance with Chapter 3 of the Act at future inspections.

Telecommunications data inspection

We conducted our inspection of the Northern Territory Police on 18 May 2016. Our findings against each inspection criterion are as follows.

1. Leadership
The Northern Territory Police has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. This appears to be underpinned by the Northern Territory Police executive and senior management's commitment to develop a strong compliance framework. This was further demonstrated by the support and involvement of the Deputy Commissioner of Northern Territory Police in the introduction of compulsory and ongoing training programs to educate officers on the significant changes to Chapter 4 of the Act.
2. Planning
The Northern Territory Police has plans in place to support compliance which include: implementing enhancements to its telecommunications data request processing system to achieve and better demonstrate compliance; and developing processes to ensure that privacy is sufficiently addressed (a new requirement under Chapter 4) and the need for journalist information warrants (JIWs) is identified. The Northern Territory Police formed a 'metadata' working group comprising relevant areas in the planning stage. The Northern Territory Police has also engaged with our office, the Attorney-General's Department and other agencies accessing telecommunications data to inform its compliance framework development. Northern Territory Police staff involved in exercising powers and those responsible for Chapter 4 compliance attended a 'metadata forum' hosted by our office, which we feel demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4; however no senior leaders from Northern Territory Police attended our office's heads-of-agency 'metadata forum'.
3. Support
The Northern Territory Police reported that it is compulsory for all staff members and authorised officers involved in accessing telecommunications data to receive training in the requirements of Chapter 4. Guidance is available for staff applying for telecommunications data, such as comprehensive standard operating procedures (SOPs), telecommunications data application templates, training packs, newsletters and system prompts.

In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks.

We noted effective communication and awareness-raising within the organisation regarding compliance with Chapter 4. Changes to Chapter 4 were communicated to relevant staff widely through group discussions, the Northern Territory Police intranet, monthly newsletters, telecommunications data computer screen savers and formal training.

The Northern Territory Police demonstrates a strong compliance culture supported by a high level of personal accountability, particularly amongst authorised officers.

4. Operation

The Northern Territory Police has effective controls which are mostly automated, strong record keeping practices, experienced staff, and embedded processes. We note the Northern Territory Police's willingness to share details of its systems with other agencies.

The Northern Territory Police updates its SOPs relating to telecommunications data access as the need arises. The SOPs specifically address the requirements of Chapter 4, including JIWs and are available to anyone involved in accessing telecommunications data.

5. Performance Evaluation

We noted that there were a number of compliance processes in place to self-evaluate the effectiveness of the Northern Territory Police's compliance procedures. These processes include informal discussions between requesting officers and authorising officers about applications for telecommunications data, multiple levels of checks for prospective telecommunications data requests, reviews of daily running sheets and compliance records, reviews of rejected applications, and weekly review meetings which discuss telecommunications data when required.

Police Integrity Commission (PIC)

Stored communications inspection

We conducted our stored communications inspection of the PIC on 2 September 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Compliant, with minor administrative issues noted. We are of the view that the PIC has sufficient procedures in place to ensure that it is only dealing with lawfully accessed stored communications.
2. Has the agency properly managed accessed information?
Compliant. Nothing came to our attention to suggest that the PIC had not properly managed accessed information. We are of the view that the PIC has sufficient procedures in place for managing accessed information.
3. Has the agency properly applied the preservation notice provisions?
Compliant, with minor administrative issues noted. We note the good practices the PIC has in place to ensure that preservation notices are revoked where a condition under s 107J(1) is no longer met, which include the use of electronic reminders for each preservation notice in force.[iv]
4. Has the agency satisfied certain record keeping and reporting obligations?
Compliant. We are of the view that the PIC has sufficient record keeping and reporting practices in place.
5. Was the agency cooperative and frank?
Compliant. The PIC has continued to be open and assistive during inspections. We also appreciate the PIC's assistance in arranging for access to operational staff members during the inspection. These staff members provided us with further information regarding the policies and procedures the PIC has in place for ensuring compliance with the Act.

Telecommunications data inspection

We conducted our inspection of the PIC on 8 December 2015. Our findings against each inspection criterion are as follows.

1. Leadership
The PIC has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this is underpinned by the PIC's executive's strong commitment to achieving compliance. This was demonstrated by the executive dedicating resources where needed to enhance processes before significant changes to Chapter 4 came into effect in October 2015, including enhancements to electronic systems and a 'data retention' working group.
2. Planning
The PIC has plans in place to support compliance which include: compulsory training in the requirements of Chapter 4; embedded controls to ensure privacy considerations are sufficiently addressed (a new requirement under Chapter 4); and ways to identify when a journalist information warrant (JIW) is required. The PIC involved relevant areas in the planning stage in a formal working group (the legal, information technology, intelligence and electronic collections units). The PIC has contacted our office with queries regarding compliance with Chapter 4, and engaged with other agencies accessing telecommunications data to inform its compliance framework. Staff members involved in exercising powers and those responsible for Chapter 4 compliance have engaged in 'metadata forums' hosted by our office. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
The PIC reported that it is compulsory for all members involved in accessing telecommunications data to receive training in the requirements of Chapter 4. This training focuses on specific responsibilities within the PIC's overall compliance framework. In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessments of compliance risks. In addition to the strong support and involvement from its executive, the PIC's legal unit has been involved in the establishment of JIW protocols, and the electronic collection and intelligence units provide compliance support to investigations staff. We noted effective communications and awareness-raising within the agency regarding compliance with Chapter 4. This included multiple formal and informal

channels where issues and updates can be raised and addressed by areas involved throughout the process, such as at regular analyst meetings or via training packages.

The PIC demonstrates a strong compliance culture.

4. Operation

The PIC has strong controls in place to support compliance which are mostly automated and are also vetted by staff.

The PIC has comprehensive standard operating procedures (SOPs) on accessing telecommunications data which are updated as the need arises. These SOPs specifically address the requirements of Chapter 4 and are available to anyone involved in the process of accessing telecommunications data.

5. Performance Evaluation

We noted that there were a number of processes in place to self-evaluate the effectiveness of the PIC's compliance procedures. For example, authorised officers return applications to investigations staff if they are insufficient, recording their explanation as to why the application was denied. Administrative errors are also recorded and returned to the applicant to be rectified. Such records will assist the PIC to evaluate areas of risk and future improvement.

Queensland Police Service (QPS)

Stored communications inspection

We conducted our stored communications inspection of the QPS from 28 to 30 July 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Compliant, with one exception. At the inspection we identified one instance where restrictions applied to a stored communications warrant were not adhered to by the carrier, resulting in stored communications being supplied to the QPS which were not authorised by the warrant.[viii] The issue was not identified by the QPS during the monitoring process, nor were the unauthorised stored communications quarantined from use. As a result, the QPS may have dealt with unlawfully accessed stored communications in contravention of s 133(1)(b)(ii).[xi] The QPS has a monitoring checklist in place for ensuring that it only deals with lawfully accessed stored communications. While we commend the QPS for implementing this procedure, we believe that it could be strengthened by including a check for whether any warrant restrictions or conditions were adhered to. In response to this finding, the QPS advised that it has implemented additional checks as part of the existing dissemination process.
2. Has the agency properly managed accessed information?
The QPS's destruction processes may not be compliant with s 150(1) of the Act. Under s 150(1) of the Act, if the chief officer of the agency is satisfied that a record obtained by accessing stored communications is not likely to be required, then the chief officer must cause the record to be destroyed forthwith.[xiv] We identified that copies of stored communications were retained by the QPS after the chief officer had authorised their destruction. This appears to be an oversight by the area responsible, who acknowledged this during the exit meeting for the inspection. In addition, despite one team's good practice of reminding investigators to destroy the stored communications records in their possession, we are not confident that all copies held by investigators have been destroyed. We note that investigators play a critical role in achieving compliance with s 150(1), and may need to be reminded that destruction records will be subject to inspection and public reporting by the Ombudsman.

At the time of inspection, the QPS advised it had not yet finalised its revised destructions policy. We suggested the policy reflect that investigators must destroy all copies of stored communications in accordance with s 150(1).

In response to this finding, the QPS advised that it has since refined existing destructions procedures to ensure the destruction of all copies of accessed information.

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

Compliant, though in two self-disclosed instances we were unable to determine compliance with the mandatory revocation requirements under s 107L(2)(a)(ii) of the Act.[iv]

In both instances, the compliance team had contacted investigators for information twice, however, no response was received. Again, we note the critical role that investigators play in achieving legislative compliance.

In addition, we identified three historic preservation notices which had not been given by officers nominated under s 110 of the Act.[vii] This has been an ongoing issue for the QPS.

In response to this issue, the QPS acknowledged that there is a potential conflict between its existing delegation under s 110 and the issuing of historic notices under s 107M.[v] The QPS advised that it has requested legal advice in relation to the revocation of the existing delegation. This advice is currently pending.

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

Compliant.

We are of the view that the QPS has sufficient record keeping and reporting practices in place.

5. Was the agency cooperative and frank?

The QPS has continued to be open and assistive during inspections. We also appreciate the transparency of QPS officers in disclosing potential compliance issues.

Telecommunications data inspection

We conducted our inspection of the QPS on 16 July 2016. Our findings against each inspection criterion are as follows.

1. Leadership
The QPS has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this is underpinned by the QPS executive's active approach to achieving compliance. This was demonstrated by the initial restriction of authorised officer numbers until a comprehensive compliance framework was developed and implemented, and formal communications from the Deputy Commissioner and senior management about the new requirements of Chapter 4 and the resulting procedural changes.
2. Planning
The QPS has plans in place to support compliance which include: general communication and training on compliance objectives; compulsory training in the specific requirements of Chapter 4 for all authorised and requesting officers; weekly state-wide communiques in the lead up to, and immediately following, significant changes to Chapter 4 which came into effect in October 2015; checklists for authorised officers and guidance sheets for investigators; and processes to identify circumstances in which journalist information warrants (JIWs) may be required. The QPS involved relevant areas in the planning stage (each area responsible for managing telecommunications data requests, investigations, legal and information technology) as part of a formal 'metadata working group'. The Acting Assistant Commissioner, QPS staff involved in exercising powers and those responsible for Chapter 4 compliance engaged in 'metadata forums' hosted by our office. The QPS also invited our office to meet and discuss queries regarding compliance with Chapter 4. We feel that this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
The QPS reported that it is compulsory for all investigations staff seeking access to telecommunications data and authorised officers to receive face-to-face training in the requirements of Chapter 4. In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks.

After significant changes to Chapter 4 came into effect in October 2015, the QPS executive temporarily restricted the power to authorise access to telecommunications data to Detective Inspectors, Detective Superintendents and State Duty Officers at the Brisbane Police Communications Centre. We believe this decision supports the QPS to ensure the requirements of Chapter 4 are carefully considered.

We noted effective awareness raising strategies within the agency regarding compliance with Chapter 4. This included timely training and dissemination of relevant information, including updates to, and distribution of, processing guides, guidance documents and comprehensive standard operating procedures regarding the requirements of Chapter 4.

The QPS demonstrates a strong compliance culture.

4. Operation

The QPS's controls are not entirely automated, and rely on the skills and experience of staff and embedded processes. For example, two areas within QPS are responsible for administering telecommunications data requests; officers within these areas perform quality assurance checks before provisioning an authorisation on a carrier. In addition, the legal unit must be engaged if a JIW may be required. The QPS has automated controls for prospective telecommunications data authorisations which prevent it from receiving content inadvertently. The QPS also has a corporate database which assists it to meet its record-keeping obligations under Chapter 4.

The QPS updates its guidance documents on accessing telecommunications data as the need arises. These publications specifically address the requirements of Chapter 4 and are available internally to anyone involved with accessing telecommunications data. The updated guides were distributed to relevant staff both prior to, and immediately after, significant changes to Chapter 4 came into effect.

5. Performance Evaluation

We noted that there were a number of compliance processes in place to self-evaluate the effectiveness of the QPS's compliance procedures. For example, managers responsible for Chapter 4 compliance will conduct reviews of prospective telecommunications data authorisations to ensure that the agency's processes are being followed. Informal discussions between authorised officers and investigators about applications also demonstrate an ongoing approach of self-evaluation and improvement at the QPS.

South Australia Police (SA Police)

Stored communications inspection

We conducted our stored communications inspection of the SA Police from 17 to 19 August 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Compliant, except in eight instances. At the inspection we identified nine instances where conditions applied to a stored communications warrant were not adhered to by the carrier, resulting in stored communications being supplied to the SA Police which were not authorised by the warrant.[ix] The SA Police identified this in one instance, however, this still resulted in eight instances where the SA Police dealt with unlawfully accessed information, contrary to s 133(1)(b)(ii).[xii] We suggested that the SA Police retrieve the relevant stored communications from the investigator(s) and quarantine those which were accessed outside of the warrant restriction. The SA Police has since advised that discs containing the relevant stored communications have been retrieved from investigators and returned to the relevant administrative team. However, one disc which was no longer in the possession of the SA Police was not able to be retrieved. We note the SA Police's advised efforts to retrieve this disc. The SA Police has monitoring and quarantining procedures in place, but checking for compliance with warrant conditions or restrictions does not appear to have been embedded into this review process. We suggested that the SA Police may wish to strengthen its procedures by introducing a monitoring checklist, either as a standalone document or by amending its pro forma for receipt of stored communications. In response to this issue, the SA Police advised that, following an internal review, new standard operating procedures were drafted outlining the actions to be undertaken when receiving stored communications. In addition, the pro forma receipt has been reviewed and now requires a member of the administrative team to acknowledge and sign in confirmation that the stored communications comply with the conditions of the warrant. We commend the SA Police for its responsiveness to this issue.

2. Has the agency properly managed accessed information?
Compliant. Nothing came to our attention to suggest that the SA Police had not properly managed accessed information, noting that no destruction activities were carried out during the inspection period. We are of the view that the SA Police has sufficient procedures in place for managing accessed information.
3. Has the agency properly applied the preservation notice provisions?
Compliant. We are of the view that the SA Police has sound procedures in place regarding preservation notices, in particular, its use of a comprehensive request form to ensure that the conditions for giving a preservation notice are met. The SA Police also has good practices in place to ensure that preservation notices are revoked when these conditions are no longer fulfilled, including revocation reminders on the request form itself and email reminders sent to the investigators.
4. Has the agency satisfied certain record keeping and reporting obligations?
Compliant. We are of the view that the SA Police has sufficient record keeping and reporting practices in place.
5. Was the agency cooperative and frank?
Compliant. The SA Police has continued to be open and assistive during inspections.

Telecommunications data inspection

We conducted our inspection of SA Police on 10 May 2016. Our findings against each inspection criterion are as follows.

1. Leadership
The SA Police has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this is underpinned by the executive's strong commitment to achieving compliance. This was demonstrated by a SA Police Assistant Commissioner distributing a memorandum on the new requirements of Chapter 4 to all authorised officers within SA Police, emphasising their personal accountability when exercising the powers.
2. Planning
The SA Police has plans in place to support compliance which include: enhancements to databases to assist with capturing the use and disclosure of telecommunications data; an onus on those applying for access to telecommunications data to sufficiently address privacy (a new requirement under Chapter 4); and a process to identify circumstances where a journalist information warrant (JIW) may be required. The SA Police involved relevant areas (legal, IT and governance) in an informal working group in the planning stage of development for its Chapter 4 compliance framework. SA Police executive, staff involved in exercising powers and those responsible for Chapter 4 compliance engaged in 'metadata forums' hosted by our office. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
The SA Police has provided specific training to authorised officers in the requirements of Chapter 4 and reported that it is finalising a training program which will be made available to all staff members accessing telecommunications data. In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks. For example, the SA Police consulted with the South Australian Crown Solicitor when developing JIW processes and incorporated liaison with the South Australia Crown Solicitor as part of its process for applying for a JIW.

We noted effective communication and awareness-raising within the agency regarding compliance with Chapter 4. This included an agency-wide communiqué shortly before and a notice in the SA Police gazette shortly after significant legislative changes to Chapter 4 in October 2015, in addition to the distribution of updated telecommunications data policies and templates. Following the inspection, the SA Police advised that it is also exploring the option of using its intranet site to raise awareness regarding Chapter 4 compliance obligations.

The SA Police demonstrates a strong compliance culture.

4. Operation

The controls that SA Police has in place to support compliance are not entirely automated and rely on the skills and experience of staff and embedded processes. For example, an officer of Inspector level or above must vet requests for telecommunications data prior their submission to an authorised officer.

The SA Police updates its policies on accessing telecommunications data as the need arises. These policies specifically address the requirements of Chapter 4 and are available to anyone involved in the process of accessing telecommunications data.

5. Performance Evaluation

We noted that there were a number of compliance processes in place to self-evaluate the effectiveness of the SA Police's compliance procedures. Two areas manage requests for telecommunications data across all SA Police; one being primarily responsible for historical data requests, the other for prospective data requests. Both of these areas are positioned to identify compliance issues as part of their quality assurance function, and address them through their coordination and training role. Additionally, informal discussions are held between investigators and authorised officers about applications, which serve to self-evaluate the effectiveness of processes by helping to identify compliance errors prior to provisioning requests onto carriers.

Tasmania Police

Stored communications inspection

We conducted our stored communications inspection of Tasmania Police from 26 to 28 April 2016. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Compliant. Tasmania Police self-disclosed one administrative issue. We are of the view that Tasmania Police has sufficient procedures in place to ensure that it is only dealing with lawfully accessed stored communications.
2. Has the agency properly managed accessed information?
Compliant, except in three instances. Tasmania Police's destruction processes may not be compliant with s 150(1) of the Act.[xiv] In three instances, stored communications records were still located on Tasmania Police's computer system, though the relevant warrants had been authorised as suitable for destruction eleven months prior. As a result, the records were not destroyed forthwith, as required by s 150(1). We also identified that investigators may be destroying copies of stored communications without the approval of the chief officer, contrary to s 150(1). We suggest that Tasmania Police take measures to improve awareness of legislative requirements – in particular, the requirement that the chief officer (or delegate) approve destructions before they occur, including the destruction of working copies. Tasmania Police could achieve this by amending its template communications to investigators, and also by providing refresher training to staff.
3. Has the agency properly applied the preservation notice provisions?
Compliant, except in two instances. We identified two instances where an ongoing preservation notice was given when another ongoing preservation notice was already in force with that carrier for the same person, contrary to s 107J(1)(e).[ii] Despite these instances, we are of the view that Tasmania Police has sufficient procedures in place regarding preservation notices. In particular, we commend Tasmania Police's effective practices (such as regularly reminding investigators about revocation requirements) to ensure that notices are revoked when the conditions under ss 107J(1)(c) and (d) are no longer met.[ii]

Nevertheless, we suggest that Tasmania Police amend its process for giving ongoing preservation notices to include a check for whether there are already any ongoing notices in force with the same carrier for the same person (or service).

In response to this finding, Tasmania Police advised that the legislative requirements for giving ongoing preservation notices have been reinforced with staff.

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

Compliant, except in three instances.

In two instances, Tasmania Police had not kept original stored communications warrants, as required by s 151(a) of the Act.[xv] In another instance, Tasmania Police was unable to demonstrate that it had kept one of the preservation notices it had given, which is a requirement of s 150A(a).[xv]

In response to this issue, Tasmania Police advised that the relevant preservation notice had been misfiled, and will be presented to our office at the next inspection.

We are of the view that Tasmania Police could strengthen its record keeping practices by amending its referencing system for stored communications warrants and preservation notices.

5. Was the agency cooperative and frank?

Compliant. Tasmania Police has continued to be open and assistive during inspections. Tasmania Police has also proactively engaged with our office outside of inspections, which we feel demonstrates a positive compliance culture.

In addition, Tasmania Police advised that a recent internal review of its administrative practices found that the issues identified at the inspection have not re-occurred to date. Tasmania Police stated that reviews of this nature will be ongoing, with a view to strengthening its compliance with the requirements of the Act.

Telecommunications data inspection

We conducted our inspection of Tasmania Police on 29 April 2016. Our findings against each inspection criterion are as follows.

1. Leadership
Tasmania Police has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that a high level of personal accountability exists at the agency and that this is underpinned by an effective quality assurance process. Authorised officers at Tasmania Police are restricted to Inspector level and above. Inspectors typically meet quarterly to discuss any issues, such as policy or legislative changes that affect requests for telecommunications data. However, Tasmania Police was unable to demonstrate whether there is executive support for compliance with Chapter 4.
2. Planning
Tasmania Police has plans in place to support compliance which include: updated templates which address privacy concerns (a new requirement under Chapter 4) and having a separate process for journalist information warrants (JIWs); some informal training on the requirements of Chapter 4 for authorised officers; and an updated intranet page with guidance on the new privacy concerns under Chapter 4. Conversations held with Tasmania Police prior to the inspection indicated that officers were not fully aware of the new requirements under Chapter 4 relating to JIWs. We note that senior executive and staff at Tasmania Police were unable to attend the 'metadata forums' and heads-of-agency forum hosted by our Office. Tasmania Police has contacted our Office and the Attorney-General's Department with queries about compliance with Chapter 4, and it has also engaged with other agencies accessing telecommunications data in preparing for its new obligations under Chapter 4. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
Based on our observations, two areas of Tasmania Police manage requests for telecommunications data; one being primarily responsible for historical data requests, the other for prospective data requests. At the inspection we noted that there appears to be limited internal communication between the two areas, which could hinder the sharing of effective compliance strategies and best practices. For example, we were advised that one area only became aware of changed requirements under Chapter 4 as a result of information received from carriers, rather than via internal communications. We suggest Tasmania Police consider

increasing internal engagement and awareness raising to encourage a consistent approach to compliance across the agency.

4. Operation

The controls Tasmania Police has in place to support compliance are not automated and rely on the skills, knowledge and experience of staff. We noted that the authorisation templates for historic and prospective telecommunications data sit with their respective areas, which in our view acts as an effective control, as investigators cannot make requests for telecommunications data except via these areas. We also noted that while all Inspectors (and their superiors) at Tasmania Police are authorised officers, in practice most requests are approved by authorised officers within the two administering areas. This restricts authorisations to a small cohort of experienced authorised officers.

Tasmania Police has standard operating procedures (SOPs), however, these documents are not regularly updated and are not relied upon by staff. We observed that officers requesting access to telecommunications data seemed aware of agency processes. Nonetheless, out-of-date SOPs increase the risk of processes being applied incorrectly or inconsistently by newer staff members.

At the time of the inspection, Tasmania Police did not have processes in place to screen prospective telecommunications data received from carriers before that information is accessed by investigators. Tasmania Police has advised that it will adopt a random and regular inspection of information from carriers, and will review the need for additional scrutiny based on the results of these internal inspections.

We noted positively that the information data management system employed by Tasmania Police is effective at restricting access to only those officers involved in an investigation and is fully auditable, which will assist with our inspections of Tasmania Police's compliance with Chapter 4.

5. Performance Evaluation

We noted that there were some compliance processes in place to self-evaluate the effectiveness of Tasmania Police's compliance procedures. For example, investigators requesting access to telecommunications data must first discuss their request with an Inspector, prior to submitting that request to an administering area. We are of the view that this additional level of control is an effective part of the overall compliance framework as it assists the agency to identify and correct errors in the first instance. The process of informal training could be of more value to Tasmania Police if information on common errors identified by Inspectors was collected and used to inform future formal training at the agency.

Remedial Action

Tasmania Police advised that the SOPs for requesting and processing requests for access to telecommunications data have been reviewed and simplified. A new draft of the SOPs is being considered before broader consultation within the agency.

In respect of the new JIW requirements, Tasmania Police conducted a review of historical telecommunications data requests to ensure that those requirements had been met.

Victoria Police

Stored communications inspection

We conducted our stored communications inspection of Victoria Police from 24 to 26 August 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Compliant, except in one instance. At the inspection we identified one instance where a restriction applied to a stored communications warrant was not adhered to by the carrier, resulting in stored communications being supplied to Victoria Police which were not authorised by the warrant.[ix] Victoria Police did not identify the issue on receiving the stored communications, and they were provided to the investigator. As a result, Victoria Police may have dealt with unlawfully accessed stored communications in contravention of s 133(1)(b)(ii) of the Act.[xi] We suggested Victoria Police retrieve the stored communications from the relevant investigator so that any unlawfully accessed product could be quarantined. In response to this issue, Victoria Police advised that the product has been retrieved from investigators and quarantined. We also suggested that Victoria Police may wish to amend its warrant checklist to include a check for compliance with any conditions or restrictions, and that it could also consider highlighting any warrant conditions or restrictions in the accompanying fax or electronic request. In response, Victoria Police advised that it has altered the warrant checklist and checking processes to better manage any warrant conditions. We will assess the effectiveness of these measures at our next inspection. Despite this instance, we are of the view that Victoria Police has good screening and quarantining procedures in place to assist with the identification of unlawfully accessed stored communications. We noted several instances where Victoria Police identified gaps or inconsistencies in the metadata for stored communications, and had contacted the carrier for confirmation that the product provided was lawful.
2. Has the agency properly managed accessed information?
Compliant, with the exception of 35 instances where stored communications records were not destroyed in accordance with s 150(1) of the Act.[xiv]

In 30 instances, stored communications records had not been destroyed forthwith, though the chief officer was satisfied that they were no longer required. We noted these destructions were impacted by a Victoria Police office relocation and staff resourcing issues.

Furthermore, we identified five instances where documents on file indicated that some stored communications records had been destroyed prior to the chief officer authorising the destruction.

Victoria Police advised that these instances were the result of a knowledge gap in investigators, which is being addressed through the dissemination of reinforced and updated information to investigation units.

Overall, we note the good practices that Victoria Police has in place for keeping track of all stored communications, being definitive about the location where accessed information is held and keeping particulars regarding each destruction. Victoria Police's practice of having two officers sign-off on each destruction (one as a witness) also strengthens its destruction process.

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

Compliant, except in one instance where a preservation notice was not revoked in accordance with s 107L(2)(a)(ii).[iv]

We note that, following this instance, Victoria Police implemented new procedures for the preservation of stored communications in certain circumstances. We will assess the effectiveness of these changes at our next inspection.

Despite this instance, we note the sound procedures Victoria Police has in place for preservation notices; in particular, the use of a comprehensive form for applications to ensure that the conditions for issuing a preservation notice are met.

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

Compliant, with the exception of an error concerning the destructions report for 2013-14. Following the inspection, Victoria Police advised that an amended version of the report was provided to the Minister in accordance with s 150(2) of the Act.[xiv]

We are of the view that Victoria Police has sufficient record keeping and reporting practices in place.

5. Was the agency cooperative and frank?

Compliant. Victoria Police has continued to be open and assistive during inspections.

We also appreciate Victoria Police's assistance in arranging access to operational staff members during the inspection. These staff members provided us with further information regarding the policies and procedures Victoria Police has in place for ensuring compliance with the Act.

Victoria Police has advised that it will continue to make the necessary amendments to processes and practices to ensure continued improvement in compliance rates.

Telecommunications data inspection

We conducted our inspection of Victoria Police on 2 May 2016. Our findings against each inspection criterion are as follows.

1. Leadership
Responsibility for compliance with Chapter 4 of the Act at Victoria Police is vested in three distinct units, however, no one area has overarching responsibility for agency compliance. We suggested to Victoria Police that executive support could be better demonstrated if senior leadership or one of the three units responsible for compliance took a lead role in aligning the compliance frameworks of each distinct unit. Despite this, at the inspection it was noted that the executive of Victoria Police is committed to compliance. This was demonstrated by the attendance of an Assistant Commissioner for Victoria Police at a heads-of-agency 'metadata forum' hosted by our office.
2. Planning
Victoria Police has plans in place to support compliance which include: prospective telecommunications data application forms and instructions which prompt officers seeking access to telecommunications data to adequately address privacy concerns (a new requirement under Chapter 4), and a standard operating procedure for journalist information warrants (JIWs). Victoria Police involved each area responsible for managing telecommunications data requests in the planning stage as part of a formal 'metadata' working group. Victoria Police were also an active participant in our 'metadata forums'. We feel this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
At the time of the inspection, Victoria Police did not have agency wide compliance training in place for officers seeking access to telecommunications data, and no additional training had been provided for authorised officers. We note, however, that at least five training sessions had been conducted for new detectives which covered the new requirements of Chapter 4. Furthermore, in approving any prospective telecommunications data requests, authorised officers must complete a detailed checklist which covers their obligations under Chapter 4. In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations, and to conduct ongoing assessment of compliance risks. For example, Victoria Police has established a project group to identify any system enhancements which may be necessary to ensure that its database (which is primarily used to apply for, approve and provision historic telecommunications data authorisations) can meet the new

requirements under Chapter 4. In addition, two of the three units (primarily responsible for administering prospective telecommunications data requests) provide ongoing advice and support on compliance to investigators.

We noted effective communication and awareness-raising within the agency regarding compliance with Chapter 4. This included an intranet announcement, and the distribution of updated templates via email and the intranet.

4. Operation

Victoria Police's controls are not entirely automated, and rely on the skills and experience of staff and embedded processes. For example, the majority of Victoria Police's prospective telecommunications data authorisations are vetted by officers within one of two relevant units, before the carrier is notified to validate the authorised officer's approval. Victoria Police's database provides automated controls for historic telecommunications data authorisations and some of the agency's prospective telecommunications data authorisations. However, this system lacks a prompt to remind officers of the new JIW requirement, which is present in Victoria Police's other processes.

5. Performance Evaluation

We noted that there were a number of informal processes in place to self-evaluate the effectiveness of Victoria Police's compliance procedures. For example, its database has a function that allows authorised officers to return requests to the applicant for further work and captures this feedback in the system. The same function is performed by officers who vet prospective telecommunications data authorisations and retain records of each rejected authorisation. These processes could be strengthened if Victoria Police had a clear leader for compliance, responsible for using this information to improve whole of agency compliance outcomes.

Remedial Action

Victoria Police advised that one Assistant Commissioner will become the senior leader designated to align the compliance framework between the three work areas that manage telecommunications data. Furthermore, Victoria Police are currently developing an online training package for all authorised officers and those members who are from time to time upgraded into authorised officer roles.

Western Australia Corruption and Crime Commission (WA CCC)

Telecommunications data inspection

We conducted our inspection of the WA CCC on 15 October 2015. Our findings against each inspection criterion are as follows.

1. Leadership
The WA CCC has demonstrated that it has clear organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act. During the inspection it was clear that this is underpinned by the WA CCC executive's strong commitment to achieving compliance. This was demonstrated by its involvement in determining the policies regarding access to telecommunications data and by formal communications from senior management, including awareness raising from the head of WA CCC operations reinforcing new obligations and updated procedures.
2. Planning
The WA CCC has plans in place to support compliance which include: compulsory training in the requirements of Chapter 4 for all investigations staff; an Aide Memoire for authorised officers which addresses privacy concerns (a new requirement under Chapter 4); an onus on officers to provide sufficient information in applications for telecommunications data; and a process to identify any circumstances where a journalist information warrant (JIW) may be required. The WA CCC involved relevant areas in the planning stage in a formal 'metadata working group' (requesting officers, records management, and the legal and governance teams). Furthermore, through fortnightly meetings of its executive, the WA CCC has an established forum to consider and approve new policies and procedures, including compliance with Chapter 4. The WA CCC has contacted our office with queries regarding compliance with Chapter 4. The Chief Executive Officer, staff members involved in exercising powers and those responsible for Chapter 4 compliance have engaged in 'metadata forums' hosted by our office. We feel that this demonstrates appropriate planning and preparedness for demonstrating compliance with Chapter 4.
3. Support
The WA CCC reported that it is compulsory for all authorised officers and investigations staff members involved in access to telecommunications data to receive training in the requirements of Chapter 4.

In our view, appropriate authority and adequate resources have been allocated to identify changes in requirements and obligations and to conduct ongoing assessment of compliance risks. Additionally, the executive's support and involvement is high; the WA CCC's legal team has been involved in planning as well as establishing JIW processes; and the governance team and records management are available to provide support to investigations staff.

The WA CCC demonstrated effective communication and awareness-raising within the agency regarding compliance with the Act. In particular, we noted timely training and awareness raising, including updates to, and distribution of, standard operating procedures (SOPs).

The WA CCC demonstrates a strong compliance culture.

4. Operation

The WA CCC has controls which are mostly automated and also rely on the skills and experience of staff and embedded processes. For example, the governance team checks applications for compliance with Chapter 4, and the legal team is engaged if a JIW may be required.

The WA CCC updates its comprehensive SOPs relating to metadata access as the need arises. These SOPs specifically address compliance requirements and are available to anyone involved in the process of accessing metadata. The updated SOPs were distributed to relevant staff by the head of WA CCC operations immediately after the significant changes to Chapter 4 in October 2015.

5. Performance Evaluation

We noted a number of compliance processes in place to self-evaluate the effectiveness of the WA CCC's compliance procedures. For example, the governance team addresses any issues in training as part of its coordination role. Informal discussions between requesting officers and authorising officers regarding applications also serve to self-evaluate the effectiveness of processes.

Western Australia Police (WA Police)

Stored communications inspection

We conducted our stored communications inspection of the WA Police from 12 to 15 October 2015. Our findings against each inspection criterion are as follows.

1. Is the agency only dealing with lawfully accessed stored communications?
Compliant. Nothing came to our attention to suggest that the WA Police had dealt with unlawfully accessed stored communications. The WA Police uses several comprehensive checklists to ensure that all legislative requirements are adhered to. We are of the view that the WA Police has sufficient procedures in place for ensuring that it is only dealing with lawfully accessed stored communications.
2. Has the agency properly managed accessed information?
Compliant. Nothing came to our attention to suggest that the WA Police had not properly managed accessed information. However, further remedial action is required in relation to a previous inspection finding on destructions. With regards to destructions, we suggested that the WA Police may wish to strengthen its procedures by reminding investigators of their obligation to return their copies of stored communications for destruction, in order to prevent the previous inspection issue from occurring in future. The WA Police advised that it now ensures that all discs are fixed with a label instructing officers as to the same.
3. Has the agency properly applied the preservation notice provisions?
Compliant, with the exception of two instances where an ongoing preservation notice was given when another ongoing preservation notice was already in force with that carrier for the same person, contrary to s 107J(1)(e).[ii] Overall, we are of the view that the WA Police's procedures with regards to preservation notices are sufficient. Nevertheless, we suggested that the WA Police may wish to broaden the checks performed before giving an ongoing preservation notice to a carrier to include the name of the subscriber, in order to avoid notices being given when another one is already in force. In response, the WA Police advised that it has included an instruction to this effect in its standard operating procedures to prevent the issue reoccurring. There were also five instances where we were unable to determine compliance with mandatory revocation requirements under s 107L(2)(a)(ii) of the Act.[iv]

In response, the WA Police advised that it previously sought guidance from the Attorney-General's Department in relation to this provision, and was advised that there was no need to revoke the preservation notice as it would expire by virtue of s 107K(b)(i) of the Act.[iii]

We agree with the advice of the Attorney-General's Department that preservation notices which expire by virtue of s 107K(b)(i) do not need to be revoked. However, in order to confirm compliance with the mandatory revocation requirements under s 107L(2), we look for evidence that the agency had maintained its intention to seek a warrant during the period that the preservation notice was in force. It is best practice to have records on file, as in the absence of such evidence, we are unable to determine compliance.

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

Compliant.

We are of the view that the WA Police has sufficient record keeping and reporting practices in place.

5. Was the agency cooperative and frank?

Compliant. The WA Police has continued to be open and assistive during inspections.

We also appreciate the WA Police's assistance in arranging for access to operational staff members during the inspection, who provided us with further information regarding the policies and procedures the WA Police has in place for ensuring compliance with the Act.

The WA Police advised that its standard operating procedures with regards to stored communications have been updated to reflect the issues raised through the inspection, and all officers have been made aware of the findings in this report.

Telecommunications data inspection

We conducted our inspection of the WA Police on 14 October 2015. Our findings against each inspection criterion are as follows.

1. Leadership
The WA Police has demonstrated that it has organisational roles and responsibilities in place to achieve compliance with Chapter 4 of the Act, which are vested in three distinct units. As no one area has overarching responsibility for agency compliance, the WA Police appears to lack a clear compliance leader. At the inspection we noted awareness-raising on the part of the WA Police's executive, specifically an agency-wide broadcast issued at the direction of an Acting Assistant Commissioner, shortly before significant changes to Chapter 4. However, the WA Police's compliance framework would benefit from further involvement from senior leadership.
2. Planning
The WA Police has plans in place to support compliance which include: authorised officer-specific awareness raising and training, including compulsory authorised officer declarations; prospective telecommunications data request templates which specifically address privacy concerns (a new requirement under Chapter 4); and standard operating procedures (SOPs) which provide guidance on journalist information warrant processes. At the time of our inspection, the WA Police's processes for access to historic telecommunications data did not reflect the new privacy requirements under Chapter 4. However, in response to this issue, the WA Police advised that historic authorisation templates have been amended to ensure that privacy concerns will be properly considered by authorised officers and that this can be demonstrated in the future. We note the WA Police's responsiveness to this issue. Individual areas were involved in planning a 'metadata' compliance framework, however this was largely done in an informal capacity. Legal and information technology areas at the WA Police approached the development of a compliance framework in a business as usual manner. We positively noted the efforts of one unit (primarily responsible for managing requests for prospective telecommunications data) to take the lead on developing an overall compliance approach for the WA Police. This unit also approached our office for advice prior to significant changes to Chapter 4 coming into effect in October 2015. However, we also noted that they had little influence on approaches taken by other areas within the agency. The WA Police's Chief Executive Officer, Acting Chief Information Officer, members of staff involved in exercising powers and those responsible for compliance with Chapter 4 engaged in 'metadata forums' hosted by our office,

which we feel demonstrates planning and preparedness from those individuals in demonstrating compliance with Chapter 4.

3. Support

The WA Police has a 'metadata' information package available to all staff. As part of its implementation of the new requirements of Chapter 4, authorised officers are provided with the SOPs and information package, and are required to sign a declaration that they understand the new requirements of Chapter 4.

The number of authorised officers who authorise requests for telecommunications data on a regular basis is sufficiently small to enable those officers to become very experienced in performing their part in the overall compliance framework.

In our view, appropriate authority and adequate resources had not been allocated to identify changes in requirements and obligations, which led to the WA Police's processes for access to historic telecommunications data not reflecting the new privacy requirements under Chapter 4. The WA Police may wish to focus its attention in this area.

The WA Police is working to increase compliance awareness within the agency. We suggest that it works to increase communication between all areas involved in applications for access to prospective and historic telecommunications data, so that best practices may be shared throughout the agency.

4. Operation

The WA Police's controls are not automated but heavily reliant on the skills and experience of staff as well as embedded processes captured in both formal and informal SOPs.

The WA Police provides SOPs to those accessing telecommunications data, however these could more specifically address the requirements for accessing historic telecommunications data.

5. Performance Evaluation

We noted that there were a number of processes in place to self-evaluate the effectiveness of the WA Police's compliance procedures. These processes include multiple levels of quality assurance prior to provisioning both historic and prospective authorisations onto carriers. We note that one unit keeps records of instances where applications were rejected prior to being authorised. In our view, this is a good practice which could be used to inform training of staff on areas of risk and for improvement, and could also be applied throughout the agency.

In relation to receiving information in error, or outside the authority of authorisations, we note that the WA Police could improve its processes by raising awareness of the need to check results and quarantine information if necessary.

Remedial Action

The WA Police advised that an Assistant Commissioner has taken on the role of responding to the areas of potential improvement identified by our office.

It also advised that templates and procedures have been revised to require the authorised officer to consciously consider the legislative requirements for approval. It also notes that the practice of recording the decisions (including any rejections) has been improved and is now standard practice across all units.

The WA Police acknowledged the need for improved communication to authorised officers regarding compliance awareness across all areas. It advised that, since the inspection, improved SOPs and training have been implemented for authorised officers. In addition, the WA Police has communicated Chapter 4 requirements to all operational police and has demanded strict compliance for requests for telecommunications data.

The WA Police notes that these measures have helped ensure a standardised approach to requests for telecommunications data.

Endnotes

[i] **Domestic preservation notices**

Under s **107H(1)**, an issuing agency may give a carrier a written notice (a domestic preservation notice) requiring the carrier to preserve, while the notice is in force, all stored communications that:

(a) relate to the person or telecommunications service specified in the notice; and
(b) the carrier holds at any time during:
    (i) the period that starts at the time the carrier receives the notice and ends at the end of the day the carrier receives the notice (in which case the notice is an historic domestic preservation notice); or
    (ii) the period that starts at the time the carrier receives the notice and ends at the end of the 29th day after the day the carrier receives the notice (in which case the notice is an ongoing domestic preservation notice).

However, s **107H(2)** provides that the agency can only give the notice if the conditions in subsection 107J(1) are satisfied.

Section **107H(3)** provides that the notice can only specify:

(a) one person; or
(b) one or more telecommunications services; or
(c) one person and one or more telecommunications services.

[ii] **Conditions for giving domestic preservation notices**

Section **107J(1)** provides that a domestic preservation notice may be given under s 107H(1) if:

(a) the issuing agency is:
    (i) for an historic domestic preservation notice—a criminal law-enforcement agency; and
    (ii) for an ongoing domestic preservation notice—a criminal law-enforcement agency that is an interception agency; and
(b) the agency is investigating a serious contravention; and
(c) the agency considers that there are reasonable grounds for suspecting that, in the relevant period for the notice, there are stored communications in existence, or stored communications might come into existence, that:
    (i) might assist in connection with the investigation; and
    (ii) relate to the person or telecommunications service specified in the notice; and
(d) the agency intends that if, at a later time, the agency considers that the stored communications would be likely to assist in connection with the investigation, then the agency will apply for a stored communications warrant (or a telecommunications interception warrant) to access those communications; and
(e) for an ongoing domestic preservation notice—there is not another ongoing domestic preservation notice in force that:
    (i) was given by the agency to the same carrier; and
    (ii) specifies the same person or telecommunications service.

[iii] **When a domestic preservation notice is in force**

Section **107K** provides that a domestic preservation notice:

(a) comes into force when the carrier receives it; and
(b) ceases to be in force at the earliest of the following times:
    (i) the end of the period of 90 days, starting on the day the carrier receives it;
    (ii) if the notice is revoked under section 107L—when the carrier receives notice of the revocation;
    (iii) if a Part 2-5 warrant or stored communications warrant authorising access to the stored communications covered by the notice is issued in relation to the issuing agency—when the warrant ceases to be in force;
    (iv) if a Part 2-2 warrant authorising access to the stored communications covered by the notice is issued in relation to the issuing agency—the end of the period of 5 days after the day the warrant was issued.

[iv] **Revoking a preservation notice (domestic or foreign)**

Under s **107L(2)(a)**, an issuing agency must revoke a domestic preservation notice if:

(i) the condition in paragraph 107J(1)(b) or (c) is no longer satisfied, or
(ii) the agency decides not to apply for a stored communications warrant or Part 2-5 (telecommunications interception) warrant to access the stored communications covered by the notice.

Under s **107R(1)**, if:

(a) a foreign country makes a request under section 107P to preserve stored communications that are held by a carrier; and
(b) in response to the request, the Australian Federal Police gives a foreign preservation notice to the carrier in relation to those stored communications under subsection 107N(1); and
(c) during the period of 180 days starting on the day the carrier was given the notice, the foreign country did not make a request to the Attorney-General under paragraph 15B(d) of the *Mutual Assistance in Criminal Matters Act 1987* to arrange for access to those communications

then the Australian Federal Police must, by the third working day after the end of that period, revoke the preservation notice by giving the carrier to whom it was given written notice of the revocation.

[v] **Persons who may give domestic preservation notices on an agency's behalf**

Under s **107M(1)**, a historic domestic preservation notice may only be given on behalf of a criminal law-enforcement agency by a person who may, under s 110, apply on the agency's behalf for a stored communications warrant to access the stored communications covered by the notice.

Under s **107M(2)**, an ongoing domestic preservation notice may only be given by an authorised officer of a criminal law-enforcement agency that is also an interception agency.

[vi] **Prohibition on access to stored communications**

Section **108(1)** provides that a person commits an offence if:

(a) the person:
  (i) accesses a stored communication; or
  (ii) authorises, suffers or permits another person to access a stored communication; or
  (iii) does any act or thing that will enable the person or another person to access a stored communication; and
(b) the person does so with the knowledge of neither of the following:
  (i) the intended recipient of the stored communication;
  (ii) the person who sent the stored communication.

[vii] **Persons who may apply for stored communications warrants on an agency's behalf**

Section **110(1)** provides that a criminal law-enforcement agency may apply to an issuing authority for a stored communications warrant in respect of a person.

Section **110(2)** provides that an application for a stored communications warrant must be made on the agency's behalf by:

(c) if the agency is referred to in subsection 39(2)—a person referred to in that subsection in relation to that agency, or
(d) otherwise:
  (i) the chief officer of the agency, or
  (ii) an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency nominated under subsection (3).

Under s **110(3)**, the chief officer of the agency may, in writing, nominate for the purposes of subparagraph (2)(b)(ii) an office or position in the agency that is involved in the management of the agency.

[viii] **Issuing of stored communications warrants**

Section **116(1)(c)** provides that an issuing authority to whom a criminal law-enforcement agency has applied for a stored communications warrant in respect of a person may, in his or her discretion, issue such a warrant if satisfied that there are reasonable grounds for suspecting that a particular carrier holds stored communications:

(i) that the person has made; or
(ii) that another person has made and for which the person is the intended recipient.

[ix] **What stored communications warrants authorise**

Section **117** provides that a stored communications warrant authorises access, subject to any conditions or restrictions that are specified in the warrant, to a stored communication:

(a) that was made by the person in respect of whom the warrant was issued, or
(b) that another person has made and for which the intended recipient is the person in respect of whom the warrant was issued

and that becomes, or became, a stored communication before the warrant is first executed in relation to the carrier that holds the communication.

[x] **Duration of stored communications warrants**

Section **119(1)** provides that a stored communications warrant will remain in force:

(a) until it is first executed, or

(b) until the end of the period of 5 days after the day on which it was issued

whichever occurs sooner.

[xi] **Exercise of authority conferred by warrant**

Section **127(1)** provides that the authority of a stored communications warrant may only be exercised by a person in relation to whom an approval under subsection (2) is in force.

Under s **127(2)**, the chief officer of the agency, or an officer of the agency appointed under subsection (3), may approve officers or staff members (or classes of officers or staff members) of the agency or another agency to exercise the authority conferred by warrants (or classes of warrants) issued to the agency.

Under s **127(3)**, the chief officer of a criminal law-enforcement agency may appoint in writing an officer of the agency to be an approving officer for the purposes of subsection (2).

[xii] **Dealing with accessed information**

Section **133(1)(b)(ii)** sets out a general prohibition on dealing with information obtained by accessing a stored communication unlawfully (in contravention of s 108(1)).

[xiii] **Communicating information to the agency**

Section **135(1)** provides that an employee of a carrier may communicate information obtained by accessing stored communications under a stored communications warrant to:

(a) the officer of the criminal law-enforcement agency who applied for the warrant on the agency's behalf; or

(b) an officer of the agency in relation to whom an authorisation under subsection (2) by the chief officer of the agency is in force in relation to the warrant.

Under s **135(2)**, 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.

[xiv] **Destruction of records**

Under s **150(1)**, if

(a) information, or a record, that was obtained by accessing a stored communication (whether or not in contravention of subsection 108(1)) is in a criminal law enforcement agency's possession; and

(b) the chief officer of the agency is satisfied that the information or record is not likely to be required for a purpose referred to in subsection 139(2) or 139A(2);

the chief officer must cause the information or record to be destroyed forthwith.

Section **150(2)** provides that the chief officer must, as soon as practicable, and in any event within 3 months after each 30 June, give to the Minister a written report that sets out the extent to which information and records were destroyed in accordance with this section.

[xv] **Obligation to keep records**

Under s **150A**, an agency is required to keep:

(a) each preservation notice given by the agency
(b) each instrument revoking such a notice, and
(c) a copy of each certificate issued under s 107U(1) by a certifying officer of the agency.

Under s **151**, an agency is required to keep:

(a) each stored communications warrant issued to the agency
(b) each instrument revoking such a warrant
(c) a copy of each certificate issued under subsection 130(1) by a certifying officer of the agency
(d) each authorisation by the chief officer under subsection 135(2), and
(e) particulars of the destruction of information and records that the chief officer has caused in accordance with section 150.

Appendix A – Telecommunications data inspection criteria - inspections conducted in 2015-16.

AS ISO 19600:2015 – Compliance Management Systems
Leadership
How has the agency's senior leadership been involved in the implementation of changes to the *Telecommunications (Interception and Access) Act 1979* (the Act) and what (if any) is their involvement in the process of exercising metadata powers?
Planning
What action has the agency taken in the lead up to the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*, which commenced on 13 October 2015?
Support
What support is provided to agency staff who exercise metadata powers?
Operation
How well have compliance obligations been integrated into the agency's practices and what controls have been implemented to ensure compliance?
Performance evaluation
What is the agency's ability to monitor and improve its compliance with Chapter 4 of the Act?
Improvement
As this was the first round of inspections, this criterion was not assessed during 2015-16.

Appendix B – Stored communications inspection criteria - inspections conducted in 2015-16.

Objective: To determine the extent of agencies' compliance with Chapter 3 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

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

1.1 Were stored communications lawfully accessed?

Process checks:

- What are the agency's policies and procedures regarding applications for a stored communications warrant?
- What are the agency's policies and procedures for ensuring that stored communications have been lawfully accessed by the carrier, including monitoring practices?
- What are the agency's policies and procedures regarding quarantining stored communications that appear to have been unlawfully accessed?

Record checks in the following areas:

- Whether the agency applied to an eligible issuing authority
- Whether a connection can be established between the person listed on the warrant and the relevant telecommunications service
- Whether a stored communications warrant in relation to the same telecommunications service as a previous stored communications warrant was applied for in accordance with s 119(5) of the TIA Act
- Whether the authority of the warrant was exercised in accordance with s 127 of the TIA Act
- Whether warrant conditions and restrictions had been adhered to
- Whether stored communications provided by the carrier were authorised by the warrant
- Whether the agency quarantined all stored communications that did not appear to have been lawfully accessed.

2. Has the agency properly managed accessed information?

2.1 Were accessed stored communications properly received and dealt with?

Process checks:

- What are the agency's policies and procedures for receiving accessed stored communications in the first instance?
- What are the agency's policies and procedures regarding the destruction of stored communications in its possession?

Record checks in the following areas:

- Whether stored communications were received in accordance with s 135 of the TIA Act
- Whether accessed stored communications were destroyed in accordance with s 150 of the TIA Act.

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

3.1 Did the agency properly apply for preservation notices?

Process checks:

- What are the agency's policies and procedures regarding applications for preservation notices?

Record checks in the following areas:

- Whether the agency was authorised to give the preservation notice
- Whether the preservation notice only requested preservation for a period permitted under legislation.

3.2 Did the agency properly give preservation notices?

Process checks:

- What are the agency's policies and procedures regarding the giving of preservation notices?

Record checks in the following areas:

- Whether the preservation notice was only issued after the relevant conditions had been met
- Whether the preservation notice was given by an authorised officer.

3.3 Did the agency revoke preservation notices when required?

Process checks:

- What are the agency's policies and procedures regarding the revocation of preservation notices?

Record checks in the following areas:

- Whether the preservation notice was revoked in the relevant circumstances.

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

4.1 Were certain records properly kept?

Process checks:

- What are the agency's processes to ensure that it satisfies its record keeping obligations?

Record checks in the following areas:

- Whether the agency has kept each record as required under Division 1 of Part 3-5 of the TIA Act.

4.2 Did the agency give the Minister a written report on destructions as required under s 150(2)?

Record checks in the following areas:

- Whether the agency has given the Minister a written report in accordance with s 150(2) of the TIA Act.

Was the agency cooperative and frank?