

**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 2017 to 30 June 2018

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

March 2019

**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 2017 to 30 June 2018

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

March 2019

ISSN 2207-4678 (Print)

ISSN 2207-4686 (Online)

© Commonwealth of Australia 2019

The Commonwealth owns the copyright in all material produced by the Ombudsman.

With the exception of the Commonwealth Coat of Arms, the Office of the Commonwealth Ombudsman's logo, any material protected by a trade mark, and where otherwise noted, all material presented in this publication is provided under a Creative Commons Attribution 4.0 licence.

The details of the relevant licence conditions are available on the Creative Commons website (creativecommons.org/licenses/by/4.0/deed.en) as is the full legal code for the CC BY 4.0 licence.



The Commonwealth's preference is that you attribute this report and any material sourced from it using the following wording:

Source: Licensed from the Commonwealth Ombudsman under a Creative Commons 4.0 licence. This report is available from the Commonwealth Ombudsman website at www.ombudsman.gov.au.

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are set out on the It's an Honour website www.itsanhonour.gov.au.

Contact us

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

Commonwealth Ombudsman

Level 5, 14 Childers Street

Canberra ACT 2600

Tel: **1300 362 072**

Email: ombudsman@ombudsman.gov.au

Contents

Executive summary	1
Summary of telecommunications data findings	2
Summary of stored communication findings.....	2
Introduction	4
Spotlight issues	7
Inspection findings.....	12
Results of telecommunications data inspections conducted in 2017–18	12
Telecommunications data: progress since 2016–17	12
Telecommunications data: response to recommendations	13
Telecommunications data: key issues for 2017–18	14
Telecommunications data: good practices	30
Results of stored communications inspections conducted in 2017–18	31
Stored communications: progress since 2016–17	31
Stored communications: response to recommendations	32
Stored communications: key issues for 2017–18	32
Stored communications: good practices	43
Agency findings for 2017–18	45
Appendix A - Telecommunications data inspection criteria: 2017–18.....	86
Appendix B - Stored communications inspection criteria: 2017–18	90

Executive summary

This report presents the results of inspections conducted by the Office of the Commonwealth Ombudsman (the Office) under s 186B of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) from 1 July 2017 to 30 June 2018. These inspections examined agency records relating to telecommunications data and stored communications for the period 1 July 2016 to 30 June 2017.¹

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

Telecommunications data, also known as metadata, is information about a communication, but does not include the content or substance of that communication. Agencies have the power to internally authorise access to this information. However, if an agency wishes to access telecommunications data that will identify a journalist's information source, the agency must apply to an external issuing authority for a warrant.

Stored communications are communications that have already occurred and are stored on a carrier's systems—they contain the content of the communication. An agency must apply to an external issuing authority for a warrant to access stored communications. Before a warrant is issued, 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 law enforcement. A person who has been subject to the use of these powers will not be aware of their use, and therefore, will not be in a position to make a complaint. Instead, the Office provides independent oversight by conducting inspections of each agency that has exercised these powers during the relevant period. At these inspections, we assess whether agencies' use of the powers complies with the legislation.

In addition to assessing compliance, we enhance transparency and public accountability by reporting our findings to the Minister for Home Affairs (the Minister) who must then make the report public.

As a result of our 2017–18 inspections, we formed the view that agencies were generally exercising their powers to access stored communications and telecommunications data appropriately. Agencies had frameworks in place to ensure appropriate access to intrusive powers and these frameworks appeared to be working as intended. Agencies also

¹ Certain aspects of our assessment require us to examine particular records outside this period in order to capture processes as they are currently being applied.

demonstrated a commitment to compliance and responded appropriately to compliance issues. Our Office also identified a reduction in the number of problems being identified, which indicates that agencies' remedial actions have been effective.

An inspection may identify a range of issues including minor administrative errors, instances of serious non-compliance and systemic issues. In reports to agencies the Ombudsman may make suggestions for improvement or make formal recommendations if an issue is sufficiently serious or the agency has not appropriately addressed a previously identified problem.

In the 37 inspections we conducted under the TIA Act during 2017–18, we made only one recommendation.

Summary of telecommunications data findings

During our 2017–18 inspections, agencies demonstrated a high level of compliance with the TIA Act and we identified fewer problems than in 2016–17. We noted good levels of transparency and accountability and strong compliance cultures, which are important in mitigating the risk of relying on an individual's diligence to achieve compliance. However, we identified non-compliance in a number of key areas including:

- authorisations that were improperly made
- an inability to sufficiently demonstrate required privacy considerations
- access to unauthorised telecommunications data
- statistics and reporting
- record-keeping.

All agencies were receptive to our findings, recommendation and suggestions.

Summary of stored communication findings

Our 2017–18 stored communications inspections assessed agencies as generally compliant with the TIA Act. During these inspections we noted good levels of transparency and accountability and strong compliance cultures. We also noted agencies' willingness to disclose compliance issues they had identified.

Notwithstanding these positive indicators, we identified non-compliance in a number of key areas, including:

- validity of stored communications warrants
- unlawful access to stored communications

- compliance with destruction requirements
- delegation of stored communications powers.

All agencies were receptive to our findings and suggestions.

Introduction

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

The Office inspects agencies' records to assess the extent of compliance with the TIA Act when their officers use these powers. The Ombudsman is also required to report the results of those inspections to the Minister, who must then table the report in Parliament.

Access to stored communications and telecommunications data are intrusive powers afforded to agencies. Our role is to independently assess compliance with legislation to enhance transparency and public accountability.

In performing this role, the Office does not oversee carriers, however, we do liaise with carriers to understand how their practices may impact agencies' compliance.

How we oversee agencies

We apply a set of inspection methodologies consistently across all agencies. These methodologies are based on the legislative requirements of the TIA Act and are regularly updated in response to legislative amendments and changes to agency processes. This ensures we can comprehensively assess compliance.

During inspections we focus on areas of high risk and consider the impact of non-compliance, for example where there is unnecessary privacy intrusion.

We base our assessments on the records agencies make available at the inspection, interviews with relevant agency staff, processes we observe and information agency staff provide in response to any identified issues. To ensure agencies understand what we will be assessing, our Office provides a broad outline of our criteria prior to each inspection. This assists agencies to identify sources of information to demonstrate compliance. We also have coercive powers to obtain information relevant to the inspection.

We encourage agencies to disclose any instances of non-compliance and tell us about any remedial action they have taken. Our Office also provides assistance to agencies to achieve compliance by assessing policies and procedures, communicating better practices in compliance, facilitating communication across agencies and engaging with agencies outside of the inspection process.

Due to the sensitive nature of the information we inspect, part of our risk mitigation strategy is to only inspect records for authorisations and warrants that are no longer in force.

The criteria for our telecommunications data inspections can be found at [Appendix A](#) and for our stored communications inspections at [Appendix B](#).

Inspection limitations

Due to the volume of records that fall within the scope of the Office's oversight, we select a representative sample to be examined. When selecting a sample, we are guided by the Auditing Standard ASA 530 *Audit Sampling*. Prior to an inspection we ask the agency to provide us with details of the total number of records subject to the inspection. Inspection officers use this information to prepare a sample, which focuses on areas of high risk and includes at least one of each of the different types of records subject to inspection.

At inspections we assess written records, electronic records, and the policies and procedures used by the agency. We supplement this with interviews with relevant officers involved in the use of these powers. Our Office does not directly observe covert powers being applied. Instead, we assess the use of powers retrospectively, through records-based inspections.

How we report

To ensure procedural fairness, following an inspection we give agencies our preliminary inspection findings and invite them to provide comments before the report is finalised. We use these finalised inspection findings to prepare our annual report to the Minister.

In our post-inspection report we may comment on specific instances of non-compliance, as well as broader issues including the adequacy of an agency's policies and procedures or any risks to compliance. We do not generally include administrative issues or instances of non-compliance where the consequences are negligible, for example where the actions of an agency did not result in unnecessary privacy intrusion.

In reporting the results of our inspections, we are constrained by the secrecy provisions in ss 133, 181B and 182 of the TIA Act. These provisions prohibit the disclosure of certain information.

Agencies we oversee

Currently, 20 agencies have access to telecommunications data and stored communications under the TIA Act. The Minister may declare additional agencies in prescribed circumstances, however the Minister did not make any such declarations in

2016–17 (the 2017–18 inspection period covered records made from 1 July 2016 to 30 June 2017). These agencies are:

Agency	Acronym
Australian Criminal Intelligence Commission	ACIC
Australian Competition and Consumer Commission	ACCC
Australian Commission for Law Enforcement Integrity	ACLEI
Australian Federal Police	AFP
Australian Securities and Investments Commission	ASIC
Corruption and Crime Commission Western Australia	CCC (WA)
Crime and Corruption Commission Queensland	CCC (QLD)
Former Department of Immigration and Border Protection (including the Australian Customs and Border Protection Service) ²	DIBP
Independent Broad-based Anti-corruption Commission	IBAC
Former Police Integrity Commission ³	LECC
New South Wales Crime Commission	NSW CC
Independent Commission Against Corruption (New South Wales)	ICAC (NSW)
New South Wales Police Force	NSW Police
Northern Territory Police	NT Police
Queensland Police Service	QLD Police
Independent Commissioner Against Corruption (South Australia)	ICAC (SA)
South Australia Police	SA Police
Tasmania Police	TAS Police
Victoria Police	VIC Police
Western Australia Police	WA Police

² On 20 December 2017, the Department of Home Affairs (Home Affairs) was established and comprises the former DIBP. As the DIBP was still an entity during the inspection period it is referred to as such for the purposes of this report, however any suggestions or recommendations have been directed to Home Affairs.

³ On 1 July 2017, the Police Integrity Commission (PIC) was abolished and the Law Enforcement Conduct Commission (LECC) commenced operations. As the PIC was still an entity at the time the inspected records were created, it is referred to as such for the purposes of this report but any suggestions or recommendations have been directed to the LECC.

Spotlight issues

During our 2017–18 telecommunications data and stored communications inspections, we identified several notable issues, outlined below.

Spotlight issue one: access to telecommunications data outside the Telecommunications (Interception and Access) Act 1979

Division 2 of the *Telecommunications Act 1997* (the Telecommunications Act) outlines the use and disclosure offences relating to information or documents held by telecommunication carriers. Specifically, Division 2 restricts telecommunication carriers from using or disclosing telecommunications data.

Specified law enforcement agencies are able to lawfully access individuals' telecommunications data despite Division 2 prohibitions, if that data is covered by an authorisation made under the TIA Act.

Authorisations made under the TIA Act, and the use and disclosure of data accessed under such authorisations, are subject to our Office's oversight under s 186B of the TIA Act.

Our Office does not have direct oversight of Division 2 of the Telecommunications Act.⁴ We also do not have visibility of carriers' actions in response to requests for telecommunications data made without an authorisation under the TIA Act.

Nevertheless, our Office has identified a number of agencies within the scope of our oversight that have accessed telecommunications data outside an authorisation made under the TIA Act. In these instances, it appears that agencies have relied upon an alternative legislative basis, outside the TIA Act, to obtain the telecommunications data.

Our Office is not aware of any statutory external oversight of any disclosure of telecommunications data that may occur outside an authorisation made under the TIA Act.

While the Ombudsman could decide to use his own motion powers under the *Ombudsman Act 1976* (the Ombudsman Act) to examine Commonwealth agencies' access to such information, there are several reasons why these general powers may not be well-suited to providing an effective or comprehensive oversight mechanism:

⁴ At the time of the 2017–18 inspections, the Ombudsman did not have any role in overseeing the *Telecommunications Act 1997*. Amendments made to that Act by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* provided Ombudsman officers with the power to inspect and report on the use of certain industry assistance powers under Part 15. However, these powers do not provide our Office with power to examine access to information under any other part of the Telecommunications Act.

- The absence of any notification or reporting obligations for agencies means our Office does not have clear visibility of if, or when, agencies access telecommunications data outside an authorisation made under the TIA Act.
- Our Office does not have jurisdiction to examine state or territory agencies' access to such information.
- Although the Ombudsman Act provides powers for our Office to examine the actions and decisions of Commonwealth agencies, we do not have jurisdiction to investigate actions or decisions carriers may take in response.

Our Office will continue to monitor this issue at future inspections, and consider if and how we might examine alternative access to telecommunications data.

Spotlight issue two: agency cooperation

Section 186B(2) outlines the Commonwealth Ombudsman's role in conducting inspections of relevant enforcement agencies. Following notification to an agency, the Ombudsman is entitled to have 'free and full access at all reasonable times to all records of the agency that are relevant to the inspection'.

Due to difficulties we encountered at inspections at the AFP in 2017–18, we were unable to complete a full assessment of its records. Some areas of the AFP and ACT Policing assisted with inspections and demonstrated a sound understanding of our inspection role, but this understanding was not apparent in our interactions with staff outside inspection areas. As a consequence, there were several administrative obstacles that impeded inspection progress.

For example, a number of our inspection officers were not granted access to the required records until halfway through the inspection. This contributed to the Office inspecting less than half of the planned number of records relating to authorisations made under s 180 of the TIA Act.

We were also concerned by a request in the lead-up to an inspection for inspection officers to undergo security vetting by AFP Personnel Security. Our Office is an independent oversight body with legislative powers to inspect records. Inspection officers are authorised by Ombudsman delegations and have undergone vetting by the Australian Government Security Vetting Agency. Further vetting by the AFP has the potential to undermine the Office's public standing as independent and impartial.

In response to our inspection findings, the AFP advised it had reviewed its procedures to ensure inspection officers have unimpeded access to relevant records during future inspections.

Spotlight issue three: authorisations, nominations and delegations

Under the stored communications and telecommunications data provisions, there are multiple functions and actions that can only be performed under the authority of an authorisation, nomination or delegation. While these often have different purposes, they all ensure the use of these powers are limited to certain agency personnel.

The issues we identified in our inspections about people not being appropriately authorised or delegated can generally be attributed to administrative errors. In contrast to other types of administrative errors, these can have quite far-reaching and serious impacts on an agency's compliance.

For example, during the previous inspection period in 2016–17, the AFP disclosed that 116 authorisations given by ACT Policing were made by people who were not authorised. An administrative error had occurred during updates to the s 5AB(1A) authorisation that resulted in ACT Policing officers being omitted. Unaware they were no longer included on the authorisation, those officers continued to make telecommunications data authorisations. The AFP then needed to appropriately manage and restrict access to telecommunications data received under these invalid authorisations. This can be especially complicated after the information has already been communicated or disclosed.

During our 2017–18 inspection at Home Affairs, we identified instances where preservation notices were given, and stored communications warrants were applied for by a person who was not nominated to do so. This meant powers had been exercised without proper authority.

Although this was the result of a simple administrative error, it presented broader complications for Home Affairs because stored communications had been obtained without the proper authority. This presents a similar issue to that highlighted for the AFP, where the accuracy of authorisations and delegations can have significant flow-on effects.

During our 2017–18 inspection at Tasmania Police, we noted that stored communications were received from a carrier by a person who was not authorised. This ultimately impacted Tasmania Police's ability to appropriately manage the information.

At most agencies, authorisations, nominations and delegations are maintained and updated by the relevant legal sections. Often the sections exercising the powers are not directly involved in the drafting process and so may simply assume the authorisations are accurate. To mitigate the risks associated with unlawfully accessing information or data,

operational sections should instead confirm that the persons exercising the powers are appropriately authorised to do so.

Spotlight issue four: prospective authorisations left to expire

Section 180(2) states an authorised officer may authorise the disclosure of specified information or specified documents that come into existence during the period the authorisation is in force. This is referred to as a 'prospective authorisation'.

Section 180(7) of the TIA Act states that an authorised officer must revoke a prospective authorisation if he or she is satisfied the disclosure is no longer required. Our Office has identified instances across a number of agencies where prospective authorisations were left to expire, in the absence of formal revocations, where there was information to indicate that the disclosure of telecommunications data was no longer required.

At our inspection of the NSWCC, our Office identified three instances of prospective authorisations being left to expire where there was information on file which indicated the grounds for the authorisations had ceased to exist. In these three instances, no formal revocation was on file and there was nothing to indicate the authorised officer had turned their mind to whether the disclosure continued to be required.

At our inspection of NSW Police, we identified one instance where information on the record indicated the authorised officer was satisfied the disclosure was no longer required, but the authorisation was left to expire rather than being revoked.

At the Office's inspection of WA Police, we identified one instance where an authorisation in force was 'cancelled' without a formal revocation being made. Without a formal revocation, the prospective authorisation remained in force until it expired.

Our Office suggests that agencies implement and follow processes to determine whether disclosure of telecommunications data under prospective authorisations is still required. Leaving prospective authorisations to expire when the disclosure is no longer required may potentially result in unnecessary privacy intrusion.

If a prospective authorisation disclosing telecommunications data is no longer required, an authorised officer should be informed and, if satisfied, revoke the authorisation. The form of a revocation of an authorisation should comply with the requirements determined by the Communications Access Coordinator under s 183(2) of the TIA Act (CAC Determination).

Spotlight issue five: administrative errors

At several agencies we identified administrative errors, such as transposing and other typographical errors, which created risks for agencies' compliance with the TIA Act.

When conducting our compliance assessments, we examine whether the information disclosed to an agency has been obtained lawfully. We do this by comparing the telecommunications data or stored communications information obtained by the agency against the instrument providing the agency with the legal authority to do so (for example, the authorisation for the access to telecommunications data, the preservation notice given to preserve the stored communications or the stored communications warrant).

We also check whether these instruments are consistent with what the agency has specified in its application documents (for example, request forms and supporting affidavits). When conducting these checks, we have identified instances where information has been transposed across documentation, or entered into electronic systems and databases incorrectly or inconsistently. Although the majority of these administrative errors did not result in unlawful access or use of information, there were instances where agencies did obtain information unlawfully. This highlights the risk that such errors can have on an agency's compliance with the TIA Act.

Generally, agencies have established measures during each stage of their use of these covert and intrusive powers to mitigate administrative errors from occurring. Whilst human error remains a possibility, comprehensive templates, clear and accessible guidance material, and quality assurance checks can all be used to mitigate these risks.

Inspection findings

Results of telecommunications data inspections conducted in 2017–18

During 2017–18 our Office conducted inspections of 20 agencies' access to telecommunications data, covering records made from 1 July 2016 to 30 June 2017.

Telecommunications data: progress since 2016–17

During the Office's 2017–18 inspections, we monitored the remedial action taken by agencies in response to issues identified during 2016–17.

During 2016–17 agencies demonstrated a high level of compliance with the TIA Act. We noted good levels of transparency and accountability and strong compliance cultures, which are important in mitigating the risk of relying on individual officers' diligence to achieve compliance. However, we identified non-compliance in a number of key areas including:

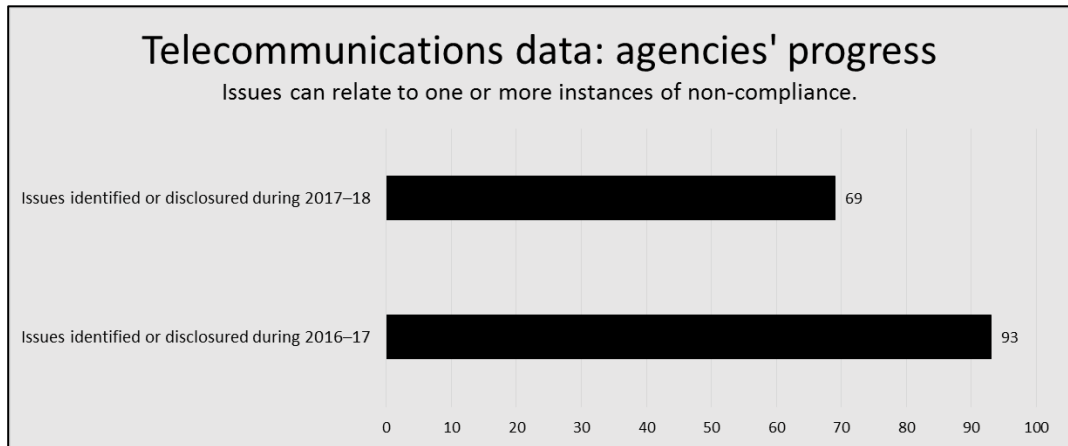
- adherence to journalist information warrant provisions
- inability to sufficiently demonstrate required privacy considerations
- access to unauthorised telecommunications data
- statistics
- record-keeping.

Overall, agencies responded appropriately to the issues raised during 2016–17. Procedures and policies were updated and remedial actions were taken in line with our suggestions and recommendations.

During 2017–18, our Office did not identify any compliance issues in relation to adherence to the journalist information warrant provisions.

Despite generally good compliance during the period, some of the key issues identified during 2016–17 were noted again during 2017–18. In some instances, this may be the result of agencies failing to take appropriate remedial action on past suggestions or recommendations. At other times, it will reflect the retrospective nature of our records based inspections, in that an agency may have implemented a fix to a problem, but we are assessing records created prior to the fix being implemented or having an appreciable effect.

Overall, through the implementation of better practice suggestions and increased agency awareness of common compliance issues, we have seen a reduction in issues being identified across the legislative regime.



Telecommunications data: response to recommendations

In 2016–17, our Office made three recommendations about issues identified during inspections.

The first recommendation was made to the AFP as a result of a non-routine inspection conducted in response to the AFP’s disclosed breach of the journalist information warrant provisions. The results of this inspection, including the recommendation, were included in our October 2017 report⁵:

AFP recommendation: *That the Australian Federal Police immediately review its approach to telecommunications data awareness raising and training to ensure that all staff involved in exercising telecommunication data powers have a thorough understanding of the legislative framework and their responsibilities under Chapter 4 of the Telecommunications (Interception and Access) Act 1979.*

AFP’s remedial actions: In September 2018 our Office conducted a follow-up inspection to assess the AFP’s remedial action in response to our October 2017 report. This report was provided to the Minister in December 2018 and is available on our website.⁶ As a result of our 2017–18 AFP inspection, we made an additional recommendation which is discussed on page 17.

⁵ The report can be accessed at: http://www.ombudsman.gov.au/data/assets/pdf_file/0021/78123/Commonwealth-Ombudsman-AFP-JIW-report-PDF-FOR-WEBSITE.pdf

⁶ The report can be accessed at: http://www.ombudsman.gov.au/data/assets/pdf_file/0034/96748/A-report-on-the-Commonwealth-Ombudsmans-inspection-of-the-Australian-Fe....pdf

The remaining two recommendations in 2016–17 were made to Home Affairs.

Home Affairs recommendation 1: *The Department of Home Affairs should implement measures to ensure it can accurately account for the number of telecommunications data authorisations it makes in any given period to enable effective oversight, and to comply with the reporting and record-keeping requirements of the Act. This should include:*

- *Implementing measures to ensure stored communications requests can be accounted for separately to telecommunications data authorisations, in particular noting the reporting obligations to the Minister under s 186 of the Act.*
- *Taking immediate action to manage the risk of inadequate technical support for the Request for Information (RFI) system, as the RFI system is heavily relied upon for reporting purposes and to assist compliance under the Act.*

Home Affairs' remedial actions: Home Affairs has established measures to ensure it can accurately account for the number of telecommunications data authorisations it makes. Specifically, Home Affairs now manually records each authorisation made. Home Affairs also advised our Office it is finalising the design of a new electronic system to more effectively meet the requirements of the TIA Act. Our Office will monitor Home Affairs' progress at future inspections.

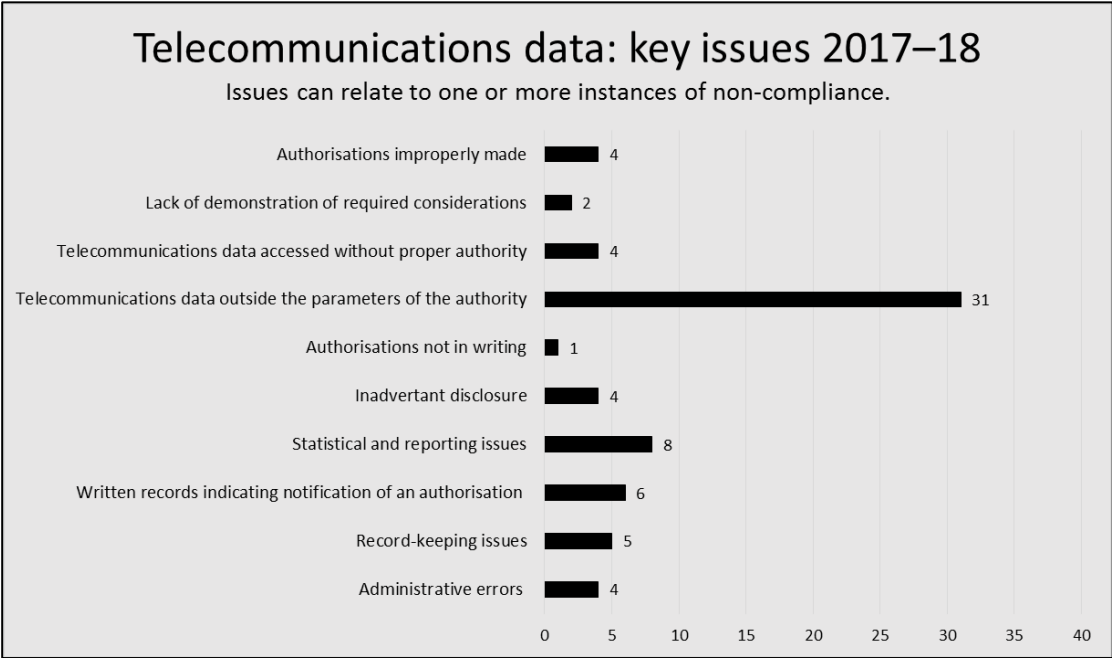
Home Affairs recommendation 2: *The Department of Home Affairs should implement measures to centrally store, and/or monitor, telecommunications data once it has been provided to investigators. In doing so, the Department of Home Affairs should be mindful of the record-keeping requirements regarding use and disclosure of telecommunications data under s 186A(1)(g) of the Act.*

Home Affairs' remedial actions: In response to this recommendation, Home Affairs developed new record-keeping practices to more effectively manage the telecommunications data it receives from carriers. Our Office will assess the effectiveness of these measures at future inspections, with a particular focus on the record-keeping requirements regarding use and disclosure of telecommunications data under s 186A(1)(g).

Telecommunications data: key issues for 2017–18

Our Office has conducted inspections of agencies' use of telecommunications data over two previous financial years. The first of these inspections were conducted in 2015–16 and were focused on understanding the policies, procedures and controls for accessing telecommunications data that were in place at each agency. The 2016–17 inspections were the first time our Office examined the records of each agencies' access to telecommunications data.

Through these two previous years of inspections, our Office has been able to gain an understanding of common areas of risk and identify better practice processes and procedures. The following key issues were identified in our 2017–18 inspections.



Authorisations improperly made

As part of our inspection assessment, our Office determines whether authorisations for access to telecommunications data have been properly made. The TIA Act stipulates a number of restrictions on the purposes for authorising access to telecommunications data. Authorisations under Chapter 4 of the TIA Act may only be made if the authorised officer is reasonably satisfied the disclosure relates to a permitted purpose including:

- the enforcement of criminal law under s 178
- locating a missing person under s 178A
- the enforcement of a law imposing a pecuniary penalty or protection of public revenue under s 179, or
- the investigation of a serious offence or an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least three years under s 180.

In addition, under s 172, authorisations for access to telecommunication data do not permit carriers to disclose the content or substance of a communication.

During 2017–18 our Office identified one instance where an authorised officer of Victoria Police made an authorisation that was not for a permitted purpose. We also identified two further instances in which Victoria Police made authorisations which requested the carrier disclose information that appeared to include content. In each of these instances, no information was received from the carrier.

We also identified one instance at Victoria Police where an authorisation was made for a period which exceeded 45 days, contrary to s 180(6)(b)(i) of the TIA Act.

We suggested Victoria Police provide targeted training to authorised officers regarding what can be authorised under the TIA Act. Our Office also suggested Victoria Police reviews its policies and procedures to ensure officers are fully informed of the requirements of the TIA Act.

Our Office will monitor Victoria Police’s remedial action on this issue at future inspections.

Demonstration of required considerations

Under s 180F of the TIA Act, before making an authorisation for telecommunications data, an authorised officer must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use of the telecommunications data is justifiable and proportionate.

Section 186A(1)(a)(i) of the TIA Act requires the chief officer to ensure documents or other materials are kept that indicate whether an authorisation was properly made, including whether all relevant considerations have been taken into account. In considering ‘other materials’, we may rely on an agency’s policies and processes, systems checks and interviews with relevant officers of the agency to inform our understanding of an agency’s processes, which are then used to assess an agency’s compliance with s 186A(1)(a)(i).

Our Office does not assess the merits of authorisations unless they are clearly contrary to the legislative thresholds. Instead, our assessments focus on whether authorised officers were provided with enough information to appropriately consider the requirements under s 180F and all other relevant considerations.

During 2017–18 our Office conducted interviews with authorised officers, requesting officers and other relevant staff to ascertain the effectiveness of processes and procedures agencies had in place to ensure authorised officers were considering the required matters.

Generally, privacy was appropriately considered by authorised officers within agencies, however we did identify two agencies that did not adequately demonstrate the required considerations had been made.

Australian Federal Police

During our inspection of the AFP, we identified 23 instances where an authorisation was made under s 178A—a provision to be used to locate a missing person—where the background information supporting the request related to the enforcement of criminal law. We also identified two authorisations granted under s 179(2)—a provision relating to enforcement of law imposing a pecuniary penalty or for the protection of public revenue—which were sought to enforce criminal law. The AFP also disclosed:

- 563 instances that authorisations were made by authorised officers but were subsequently rejected by an internal quality assurance process
- 73 instances that authorisations were notified to the carrier with errors.

We acknowledge the important role the AFP's internal quality assurance process plays in assisting the AFP's compliance with the TIA Act, but are concerned about the number of errors being made and/or not being identified by authorised officers. These errors may demonstrate a lack of appropriate consideration by authorised officers.

Our Office also identified four instances where records reflected less than one minute had lapsed between the request being sent to the authorised officer and the return response making the authorisation. Given the range of matters requiring consideration by authorised officers, this timeframe calls into question whether the requirements could have been met.

The role of the authorised officer is a critical control for ensuring telecommunications data powers are being used appropriately. We note the errors identified by our Office and disclosed by the AFP related to multiple authorised officers across a number of teams within the AFP. This means the errors cannot be attributed to an individual, team or process but, rather, indicate AFP staff do not have a well-embedded appreciation of the requirements of the TIA Act and the individual responsibility of authorised officers.

We note this was also a contributing factor to the breach of the journalist information warrant provisions, which was disclosed by the AFP in April 2017 and reported on by our Office in October 2017.

The inspection report reflected that our Office was not satisfied the AFP had demonstrated that authorised officers consistently had regard to the considerations required under the TIA Act. As a result, we made the following recommendation:

AFP recommendation: *That the Australian Federal Police implements processes to ensure authorised officers have regard to the required considerations prior to authorising access to telecommunications data under Chapter 4 of the Telecommunications (Interception and Access) Act 1979.*

In response, the AFP advised it released an online mandatory training package for authorised officers in November 2017. Authorised officers are required to complete this training annually. The AFP also released a supplementary training and reference tool, and implemented template changes which will assist the AFP in demonstrating authorised officers have regard to the required considerations.

The AFP noted that the authorisations inspected during 2017–18 were made prior to the release of this training package and it expects there will be a significant reduction in compliance issues identified at our 2018–19 inspection as a result of the mandatory training.

Following the 2017–18 inspection, the AFP has been proactive in engaging with our Office to discuss better practices and process updates to more effectively demonstrate the required considerations.

We will monitor the AFP's progress on this issue at future inspections.

Tasmania Police

Our Office also identified an issue of a similar nature during our inspection of Tasmania Police.

We understand Tasmania Police's process as follows. In the earliest stages of seeking an authorisation, a requesting officer will verbally brief a regional inspector on their request. The requesting officer may then make a statement confirming that a regional inspector has approved the request for the authorisation.

In addition to obtaining the regional inspector's approval, Tasmania Police's authorisation process also requires that all authorisations are quality assured by a specific role within Tasmania Police. The role of this specific officer is to then make the authorisation. There may be some debate within Tasmania Police about who is ultimately performing the role of the authorised officer but, based on our understanding of these processes, it seems clear all authorisations are made by this one specific role.

In practice, this has the regional inspector assuming responsibility for making the relevant considerations, but not the formal written authorisation itself.

This means there are, in effect, two distinct entities performing different aspects of the authorised officer role. However, Chapter 4 of the TIA Act does not provide for this distinction.

Before making an authorisation, the authorised officer must be satisfied any interference with a person's privacy is justifiable and proportionate, and that the disclosure is

reasonably necessary for a permitted purpose, such as the enforcement of criminal law. An authorised officer must not make an authorisation that would authorise the disclosure of information or documents of a particular person, if the authorised officer knows or reasonably believes the particular person to be a journalist or an employer of a journalist, unless a journalist information warrant is in force.

We were not satisfied that the specific role formally making each authorisation had made the relevant considerations, because they had relied on the regional inspector to make the considerations on their behalf. As the regional inspectors had largely relied on verbal briefings, there were also no records to indicate what considerations had been made at this level and whether this information was available to the officer formally making the authorisation.

As a result of this issue, our Office suggested Tasmania Police review its policies and procedures to ensure it can demonstrate relevant considerations are made by the authorised officer for each authorisation. Our Office will monitor Tasmania Police's progress in relation to this issue at future inspections.

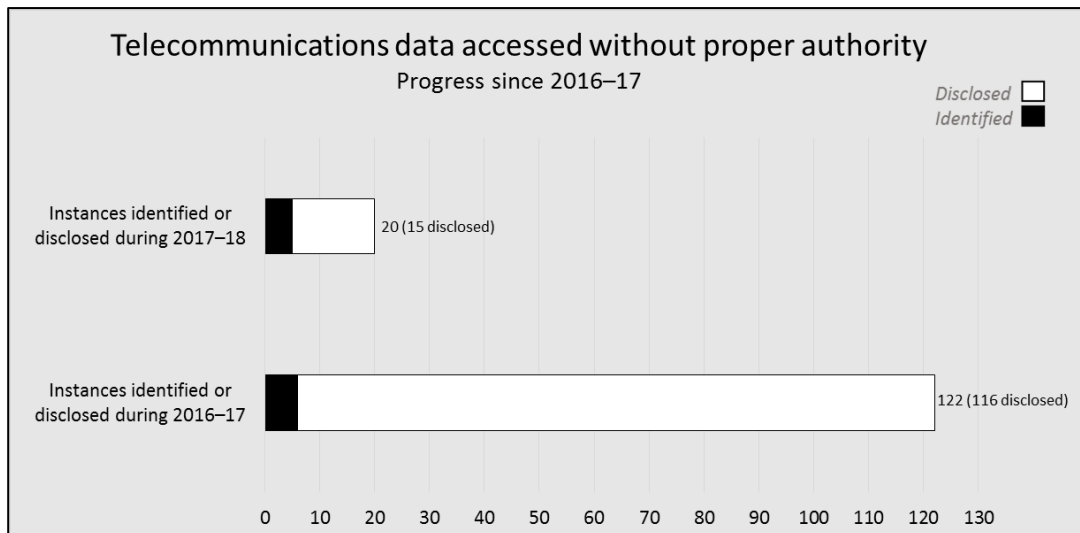
Telecommunications data accessed without proper authority

Section 5AB(1) of the TIA Act states that the chief officer of an enforcement agency may authorise, in writing, a management officer or management position to be an 'authorised officer'. Under the TIA Act, only an authorised officer may authorise the disclosure of telecommunications data.

During 2017–18 we identified a small number of instances at agencies where telecommunications data was obtained prior to, or without a valid authorisation.⁷ This occurred as a result of processes and procedures being incorrectly applied. In each instance, we were satisfied by the prompt remedial action the agency implemented.

The number of issues identified or disclosed where telecommunications data was accessed without proper authority reduced significantly between 2016–17 and 2017–18. In our 2016–17 report we explained the AFP had disclosed 116 authorisations given by ACT Policing during 2015–16 were made by people who were not authorised. The AFP's subsequent resolution of that matter is one factor in the lower number reported this year but, more generally, it also indicates agencies overall have improved their processes to mitigate these issues. We suggest agencies maintain ongoing training and awareness raising to ensure established processes are consistently complied with.

⁷ ACIC, WA Police, DIBP and ICAC (SA).



Telecommunications data outside parameters of the authority

Under the TIA Act, an authorised officer may authorise the disclosure of specified telecommunications data that “came into existence before the carrier received notification of the authorisation”. This is known as an ‘historic authorisation’. As historic authorisations only permit access to existing telecommunications data, any telecommunications data dated after the authorisation comes into force is outside the parameters of the authority.

The TIA Act also establishes that an authorised officer may authorise the disclosure of specified telecommunications data that “comes into existence during the period the authorisation is in force”. This is a ‘prospective authorisation’. A prospective authorisation comes into force at the time the carrier receives notification of the authorisation and, unless the authority is revoked, ends at the time specified in the authorisation.⁸ Any telecommunications data dated before the authorisation comes into force, after its expiry, or after it was revoked, is outside the parameters of the authority.

An agency may further limit the scope of the telecommunications data it authorises by restricting the request to a particular date range or search terms.

When conducting our compliance assessments under these sections, we take into consideration what telecommunications data the agency has specified on the authorisation and whether the telecommunications data provided by the carrier complies with those parameters.

⁸ Sections 180 and 180B of the Act.

Broadly speaking, for these types of authorisations, telecommunications data received outside the parameters of the authority can be divided into four distinct categories:

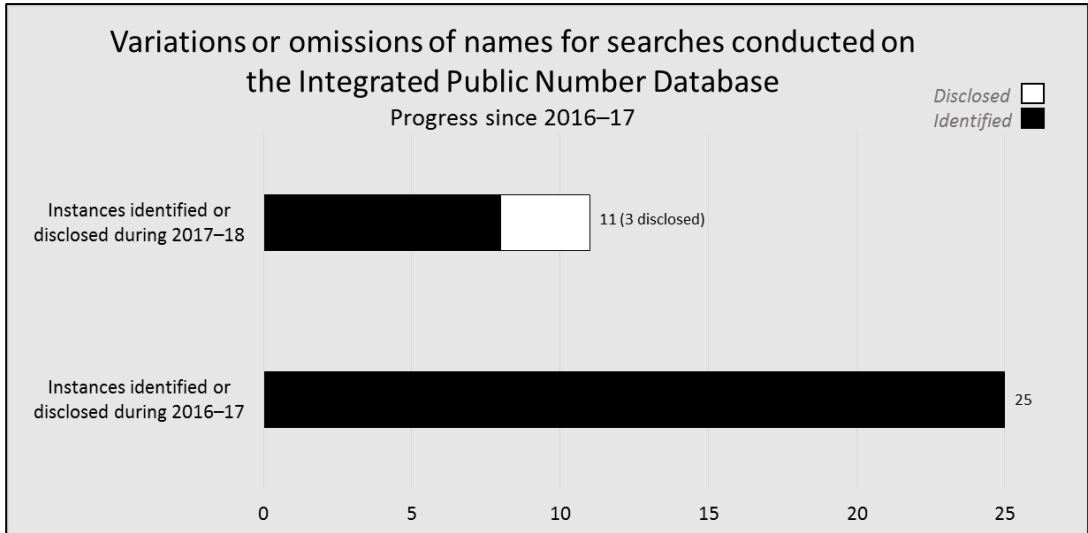
1. variations or omissions of names for searches conducted on the Integrated Public Number Database
2. telecommunications data outside the authorised period
3. telecommunications data received after revocation took effect
4. receipt of telecommunications data not specified on the authority.

1. Variations or omissions of names for searches conducted on the Integrated Public Number Database

One of the most prevalent issues during our inspections in 2016–17 related to searches of the Integrated Public Number Database (IPND) that were outside the parameters of the authority. The IPND is an industry-wide database which contains all listed and unlisted public telephone numbers. Information contained in the IPND may include the name and address of the customer, and the type of service registered to that customer.

In 2016–17 and 2017–18, our Office identified several instances where IPND searches did not match the search terms specified on the authorisations. Generally these searches either included names or versions of names not included on the authorisation (thereby increasing the privacy intrusion). In our view authorised officers should be fully aware of the particulars of each search that will be conducted under an authorisation, so they can be satisfied of the required considerations. Permutations of names and additional aliases will invariably impact upon these considerations.

The number of issues we identified relating to IPND searches reduced significantly between 2016–17 and 2017–18. This is a strong indication that remedial actions taken by agencies have been effective in mitigating reoccurrence. Agencies also disclosed instances to our Office which demonstrates their increased awareness of the issue.



2. Telecommunications data provided to agencies outside the authorised period

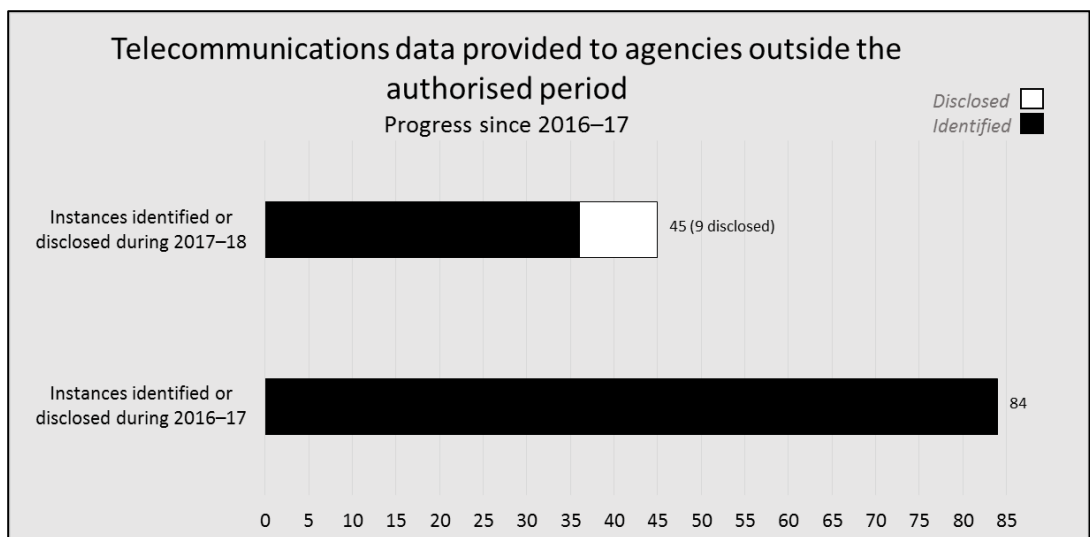
For historic authorisations, we encountered a significant number of instances in which telecommunications data obtained by agencies was either outside the date range specified on the authorisation or was dated after the carrier was notified of the authorisation. Although an agency has limited control over whether the telecommunications data the carrier provides is in accordance with an authorisation, the onus is on the agency to verify that any telecommunications data received outside the terms of the authorisation is managed appropriately. Any telecommunications data received that is outside the authorised period should be quarantined from use and disclosure. Ideally, initial screening and vetting should be undertaken as a matter of course to mitigate against the risk of using telecommunications data outside the authorised period.

For prospective authorisations we noted fewer instances where telecommunications data was received outside the authorised period, except for authorisations where telecommunications data was received after a revocation had taken effect, which is discussed in the next section.

Initial screening and vetting practices offer agencies additional assurance that they are only dealing with lawfully accessed telecommunications data. We accept vetting is not feasible in all instances, particularly where an agency accesses a significant volume of telecommunications data. It is particularly important that an agency’s processes mitigate non-compliance by ensuring those who receive, and use information from carriers are aware of the need to identify and quarantine telecommunications data which is outside

the authorised period. Generally, agencies responded appropriately to the instances identified by our Office and quarantined the relevant telecommunications data.

During 2017–18, agencies were increasingly aware of the potential for carriers to provide telecommunications data outside the authorised period. Agencies have generally established strong quality assurance processes to identify and quarantine such information. Many agencies have also implemented processes and procedures to proactively mitigate occurrence of this issue. For example, agencies can restrict requests for telecommunications data to the day before the carrier is notified of the authorisation. This process mitigates agencies from accessing telecommunications data that is dated after the carrier is notified.



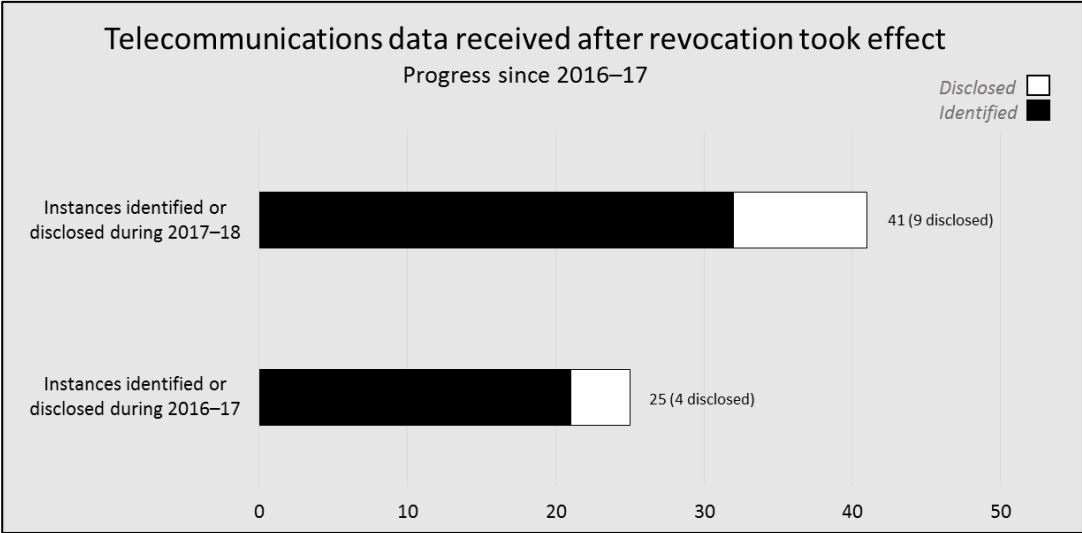
3. Telecommunications data received after revocation took effect

During our inspections, we identified risks related to the revocation of prospective authorisations. Although the legislation is silent on when a revocation takes effect, we work on the basis that it takes effect at the time the carrier is notified of the revocation, unless a date and time of effect is specified on the revocation.

Where agencies state a date and time of effect on revocation instruments, there is a risk the agency will continue to receive telecommunications data after revocation. This will usually occur as a result of a delay between the time the authorised officer signs the revocation instrument and the carrier receiving notification from the agency that the revocation has occurred. We note that, to counter this, some agencies advise the carrier of

the proposed revocation, and seek a disconnection to prevent continued access to telecommunications data, before the formal revocation is made.

This issue was also identified during our inspections in 2016–17. We anticipated instances of non-compliance attributed to this issue would decrease as a result of us highlighting it with agencies and agencies subsequently updating their procedures in response. We think it is likely the expected improvement is not yet evident because the retrospective nature of our records-based inspections means we have not yet assessed the more recent records that would have benefited from agencies’ remedial actions. We expect to see the full impact of remedial actions, and an associated decrease in the number of instances, at future inspections.



4. Obtained telecommunications data not specified on authority

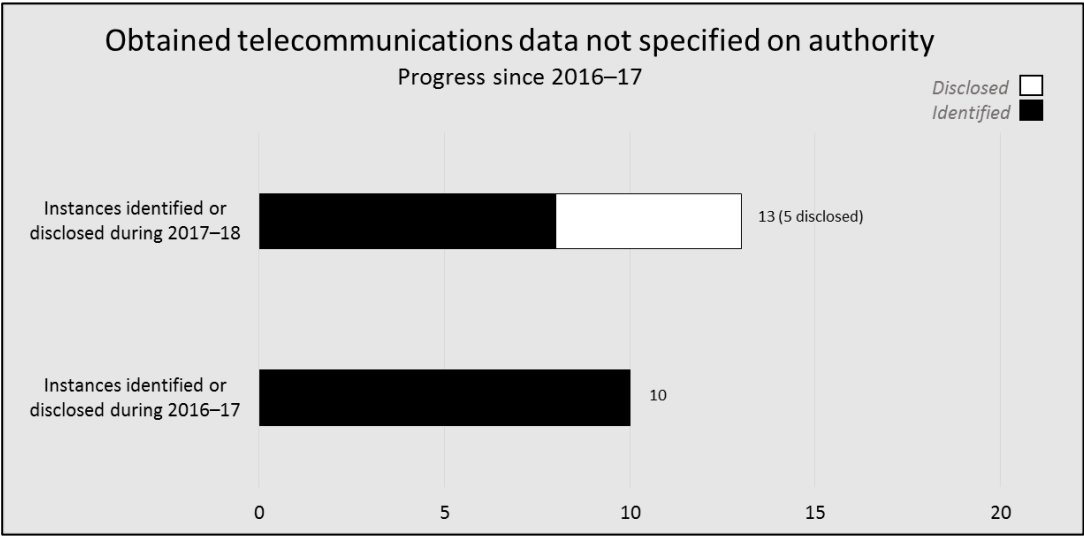
Our Office identified instances at nine agencies where carriers provided telecommunications data not specified on the authorisation. This occurred as a result of issues such as:

- Agencies accessing telecommunications data which was specified on the supporting information but had been erroneously omitted from the authorisation itself.
- Carriers providing telecommunications data the agencies had not requested.
- Transposing errors on the notification of authorisation which resulted in data being obtained which was not specified on the authority.

In two of these instances⁹, the telecommunications data provided by the carrier did not specify what telecommunications service the information related to. As a result, our Office was unable to determine whether the telecommunications data the carrier provided was within the parameters of the authority.

Quality assurance mechanisms during the authorisation process and prior to carrier notification enable agencies to mitigate the risk of receiving telecommunications data not specified on the authorisation. It is also important that agencies’ processes are geared towards mitigating this type of non-compliance by ensuring that those who receive telecommunications data are aware of the need to identify and quarantine information not specified on the authorisation.

Whilst the total number of instances identified or disclosed this year has increased compared to our previous inspections conducted in 2016–17, this is reflective of increased disclosures from agencies. This demonstrates agencies’ increased awareness of the issue.



Authorisations not in written form

In certain circumstances, an agency may need to authorise access to telecommunications data urgently. This may mean that, for example, it is operationally impractical for the agency to follow the standard procedures for seeking a written authorisation. Chapter 4 of the TIA Act has no framework to govern the use of verbal or urgent authorisations. However, s 183 of the TIA Act requires that an authorisation for telecommunications data must be in written or electronic form and must be signed by the authorised officer.

⁹ ASIC and QLD Police.

The following considerations must be made when an authorised officer decides whether to give an authorisation:

- the interference in a person’s privacy is justifiable and proportionate
- the disclosure is reasonably necessary for a permitted purpose, such as the enforcement of criminal law.

Additionally, for journalist information warrants, an authorised officer must not authorise the disclosure of the telecommunications data of a journalist or their employer for the purpose of identifying their source, unless a journalist information warrant is in force.

In the absence of any records to demonstrate these considerations, we are unable to determine that an authorised officer took into account the requisite considerations when giving the authorisation.

During 2017–18, we identified one area of Tasmania Police that was routinely exercising its telecommunications data powers without a written or electronic authorisation. The area’s standard practice at the time was for access to telecommunications data to be approved verbally.

Under s 183 of the TIA Act, an authorisation for telecommunications data must be in written or electronic form and signed by the authorised officer. Telecommunications data accessed through a verbal approval, outside a formal authorisation process, may not demonstrate the core considerations required to access telecommunications data and does not meet the requirements under s 183 of the TIA Act. As a result, all authorisations made within this specific area of Tasmania Police did not meet the requirements of the TIA Act. From April 2017, the area updated its procedures to ensure a written record is made of each authorisation. Unfortunately this approach still did not meet the form requirements under the TIA Act.

Inadvertent disclosure

Section 181B(1) of the TIA Act sets out use and disclosure offences related to telecommunications data, including disclosure about whether an authorisation under Division 4 has been, or is being sought.

Section 181B(3)(b)(ii) permits disclosure of this information if it is reasonably necessary for the enforcement of the criminal law.

During 2017–18 we identified a small number of agencies that had inadvertently disclosed it was seeking an authorisation.¹⁰ The majority of instances occurred when the agency

¹⁰ IBAC, ICAC (SA), ICAC (NSW) and ACIC.

notified the incorrect carrier about an authorisation. However in one instance IBAC disclosed to a member of the public, who was unrelated to the investigation, that an authorisation was being sought. We note IBAC's advice it took action to contain the information in that instance.

Agencies should have strong controls in place to ensure that notification of an authorisation is only provided to the person (for example, the carrier) from whom the disclosure is sought. Any inadvertent disclosures may potentially breach s 181B(1) of the TIA Act.

Statistical and reporting issues

Section 186 of the TIA Act sets out agencies' reporting obligations to the Minister. Under this section agencies must, as soon as practicable and in any event within three months after the end of the financial year, provide the Minister with a written report that sets out specific details of that agency's access to telecommunications data. This includes the number of authorisations made by an agency during the financial year.

During 2017–18 we identified a small number of agencies that had discrepancies in their statistics. This occurred for a number of reasons including:

- the type of authorisation being recorded inconsistently
- agency officers erroneously recording authorisations made
- system limitations which prevented the agency from obtaining accurate details of the total number of authorisations made.

We also identified the ACCC had provided their report to the Minister under s 186 of the TIA Act outside the specified timeframe of three months.

Generally, agencies were receptive to our suggestions and advised their processes and procedures would be updated to ensure statistical information provided to the Minister under s 186 reflects the total number of authorisations made.

Written records indicating notification of an authorisation

Under s 186A(1)(a)(iii) of the TIA Act, agencies must retain documents or other materials that indicate when a carrier is notified of an authorisation under s 184(3). In considering 'other materials', we may take into account an agency's policies and procedures.

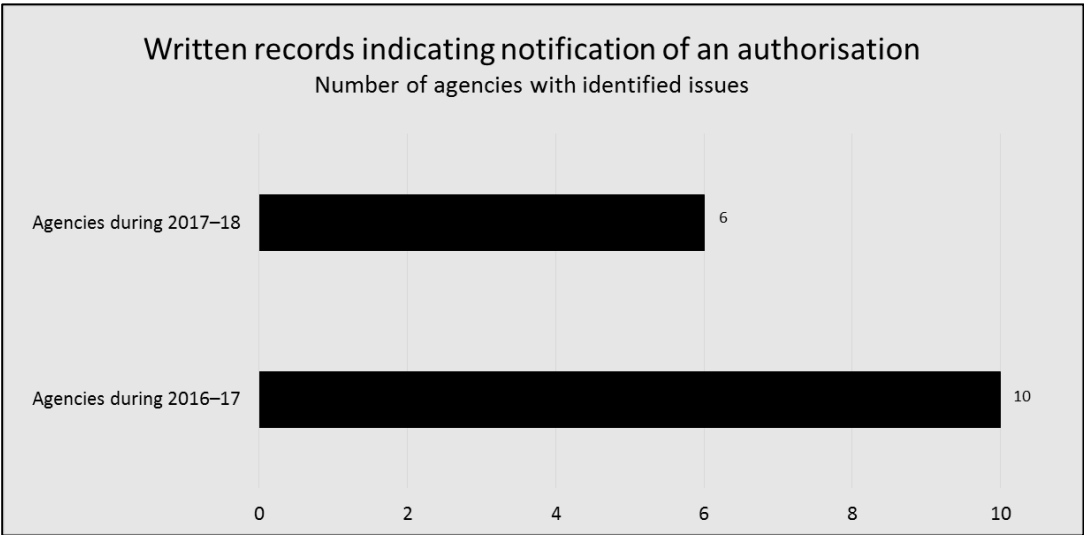
One of the most common risks we identified during our inspections was agencies not maintaining written records to indicate when notification of authorisation occurred. While it is reasonable to conclude notification would need to have occurred in order to receive

telecommunications data from the carrier, the lack of these records poses a risk that agencies may not be able to demonstrate they are accessing authorised telecommunications data.

An example of this is where an agency has made a historic authorisation requesting telecommunications data from the same day the notification of authorisation occurred. Without a written record of when notification occurred, the agency may not be able to demonstrate the telecommunications data obtained came into existence before the authorisation came into force.

With this in mind, during 2016–17 our Office suggested agencies adopt processes to keep clear written records of the date and time the carrier received notification of the authorisation.

All agencies for which this issue was identified during 2017–18 have implemented updated processes and procedures to ensure a written record of when notification occurred is retained. The issues identified during 2017–18 were also largely the result of these updated processes not yet taking effect for the records being inspected, due to the retrospective nature of our inspections. Nevertheless, our Office identified a decrease in the number of agencies where this issue was identified.



Record-keeping

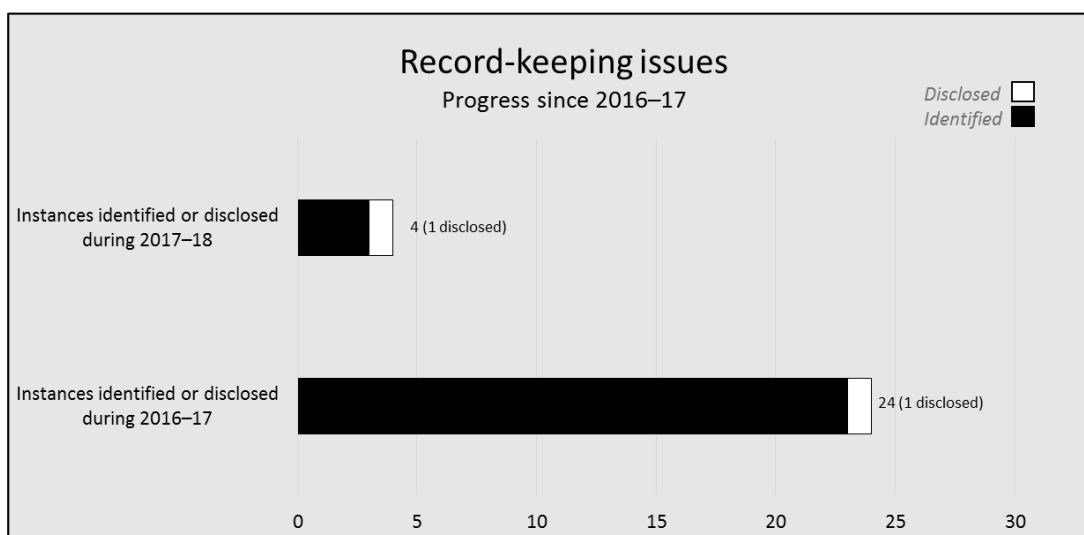
Section 186A(1)(g) of the TIA Act requires the chief officer of an enforcement agency to keep documents or other materials that indicate whether use or disclosure of telecommunications data occurred in certain circumstances. Under s 185, agencies must also retain each authorisation by an authorised officer for a period of three years beginning on the day the authorisation is made.

During our inspections, we made several findings regarding agencies being unable to provide access to, or locate the telecommunications data obtained under authorisations. In conducting our compliance assessment, we review the telecommunications data received under an authorisation to ensure it is within the parameters of the authorisation, including confirming the information is linked to the telecommunications service authorised.

Although there is no express legislative provision requiring agencies to retain accessed telecommunications data, an inability to account for the whereabouts of obtained telecommunications data may mean agencies are not able to appropriately demonstrate whether, and how, that telecommunications data was used and/or disclosed in accordance with s 186A(1)(g).

We also identified a small number of instances in which agencies could not locate the authorisation itself. In these circumstances we relied on agencies' processes and procedures to confirm the access to telecommunications data had been properly authorised prior to access.

Overall, we identified a smaller number of record-keeping issues in 2017–18 than in 2016–17.



Telecommunications data: good practices

During our inspections we examine the adequacy of agencies' policies and procedures for ensuring compliance with the TIA Act, based on information provided by the agency. This includes identifying practices that assist agencies in achieving compliance, as well as practices that pose risks to an agency. Examples of good practices, as identified during our inspections for the 2017–18 period, are outlined below.

Good practice: inter-agency cooperation and information sharing

During our inspections we observed a number of positive instances of inter-agency cooperation and information-sharing. Our Office encourages cooperation within and between agencies to facilitate sharing of common compliance issues and better practices.

By way of example, during 2017–18, WA Police established the Australian Policing Jurisdictions Teleconference Group. The objectives of this group are to share compliance issues arising from inspections, discuss common carrier issues and share knowledge and better practices.

We also note WA Police's efforts in:

- Visiting other state agencies (NSW Police and VIC Police) to observe their methods and procedures.
- Reaching out to other agencies (NT Police and QLD Police) regarding the use and disclosure of telecommunications data.

Alongside inter-agency cooperation, our Office also noted a number of agencies that demonstrated strong internal cooperation. Our Office has identified that strong internal cooperation and ongoing communication can positively assist with an agency's ability to maintain compliance. We suggest all agencies consider the mechanisms they have in place to facilitate cooperation and communication within their organisation.

Results of stored communications inspections conducted in 2017–18

During 2017–18 our Office conducted 17 inspections of agencies' access to stored communications. These inspections covered records made from 1 July 2016 to 30 June 2017.

Stored communications: progress since 2016–17

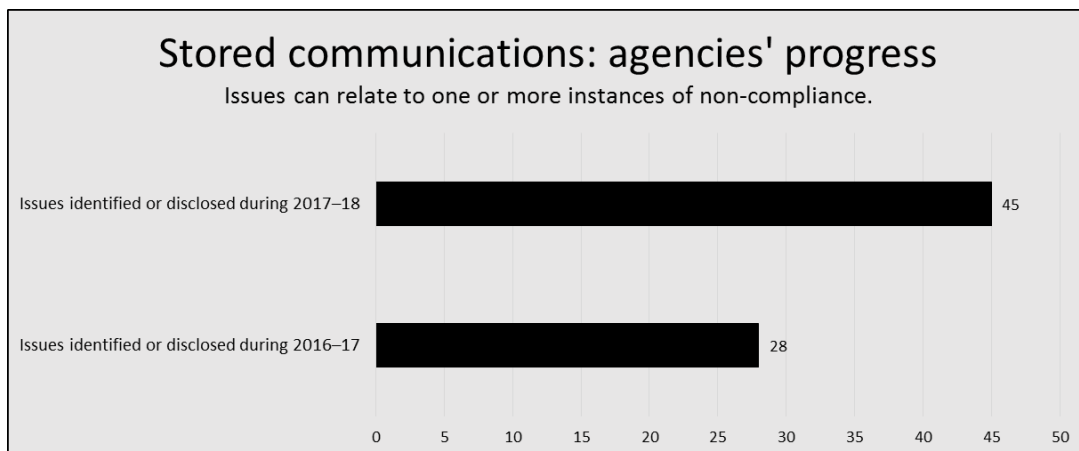
During our 2017–18 inspections, our Office monitored the remedial action agencies took in response to the key issues identified during 2016–17.

Our 2016–17 inspections assessed agencies as generally compliant with the TIA Act. During our stored communications inspections we noted good levels of transparency and accountability, and strong compliance cultures. We also noted agencies' willingness to disclose compliance issues they had identified. Notwithstanding these positive observations, we also identified non-compliance in a several areas:

- mandatory revocation requirements for preservation notices
- agencies' actions in response to receiving unlawfully accessed stored communications from carriers
- destruction requirements
- proper delegation of stored communications powers.

Overall, agencies responded appropriately to the issues raised during 2016–17. They updated procedures and policies were updated, and took other remedial action in response to our suggestions.

Despite this, some of the issues we identified during 2016–17 were identified again in 2017–18.



Stored communications: response to recommendations

Our Office did not make any recommendations about issues identified during inspections conducted in 2016–17. However, due to issues identified during 2017–18, we discussed three previous recommendations with Home Affairs.¹¹ These are discussed in the findings below.

Stored communications: key issues for 2017–18

Overall, in 2017–18 we identified an increased number of compliance issues, as well as instances where we were unable to determine compliance, compared to 2016–17.

While there was a decrease in issues about unlawfully accessed stored communications and preservation notices being left to expire, we identified an increased number of issues about destructions and annual reporting. The following are the key issues our Office identified in our 2017–18 inspections.

¹¹ At the time these recommendations were made, operational and enforcement functions were carried out by the then Australian Customs and Border Protection Service. These functions have since been incorporated into Home Affairs and, as such, the remedial action taken in response has been assessed at Home Affairs.

Stored communications: key issues 2017–18

Issues can relate to one or more instances of non-compliance.



Invalid stored communications warrant

Section 6DB sets out who is an issuing authority for the purpose of issuing stored communications warrants. Specifically, in order to be an issuing authority for the purposes of s 6DB, a person must be appointed by the Attorney-General.¹²

During 2017–18, our Office identified four stored communication warrants at Tasmania Police that were issued by a magistrate who had not been appointed as an issuing authority by the Attorney-General under s 6DB. When we identified this issue Tasmania Police advised it would quarantine the accessed stored communications.

Our Office was satisfied with the remedial actions proposed by Tasmania Police in response to this issue.

Stored communications of a victim accessed without consent

Section 116 sets out the circumstances in which an issuing authority may issue a stored communications warrant to an agency. Where an agency applies for a warrant to access the stored communications of a victim of a serious contravention under investigation, the issuing authority must be satisfied the victim is unable to consent to their stored communications being accessed or it is impracticable for their consent to be obtained.

¹² Only a judge, magistrate, a member of the Administrative Appeals Tribunal, or a legal practitioner of a federal court or of the Supreme Court of a State or a Territory can be appointed as an issuing authority for the purposes of s 6DB.

We identified two instances at Tasmania Police and one instance at NT Police where it appeared the agencies had accessed the stored communications of a victim of a serious contravention without first obtaining the victim's consent. Based on the available records, it did not appear the victim was unable to consent or it was impracticable for them to consent.

This issue has been identified in previous years at a number of agencies and continues to be an area of focus for our inspections. We have previously sought the Attorney-General's Department's (AGD) view, in its former role as the TIA Act's administrator, on the meaning of the terms 'unable' and 'impracticable' under s 116(1)(da). The AGD advised our Office a person would be deemed 'unable to consent' where, for example, they are missing and cannot be located, are incapacitated or deceased. Obtaining consent would be deemed 'impracticable' where a person's particular situation makes contacting them extremely difficult, time-consuming or expensive.

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

Better practice suggestion

Our Office also identified one instance at NSW Police where it applied for a stored communications warrant in relation to a victim's service on the basis that the person of interest had used that service. Although all stored communications accessed under this warrant were authorised, the application to the issuing authority did not explicitly address the potential privacy implications of the carrier providing stored communications which had been made by the victim and which did not relate to the investigation.

In these situations, it is best practice for agencies to ensure the application for a stored communication warrant addresses this potential risk, and highlights the controls the agency has in place to mitigate any unnecessary privacy intrusion for the victim. By including this level of detail in applications, our Office can be confident that when an issuing authority exercises their discretion to issue or not issue a stored communications warrant under s 116, they have been provided all relevant information.

Historic preservation notice given in an ongoing manner

Under s 107H of the TIA Act, there are two types of domestic preservation notices: historic and ongoing. A law enforcement agency may give a carrier a historic notice to require the carrier to preserve stored communications from the time it receives the notice until the end of that day. A law enforcement agency that is also an interception agency may give a

carrier an ongoing notice to require the carrier to preserve stored communications from the time it receives the notice until the end of the 29th day after that date.

During the inspection period, Home Affairs disclosed to us that it gave a series of 56 historic domestic preservation notices to the same carrier over consecutive periods, each relating to the same person. In our inspection we identified that it appeared Home Affairs had given 100, not 56, consecutive historic domestic preservation notices. While this practice is not strictly in breach of any legislative provision, in our view it has a similar effect to giving an ongoing preservation notice. Home Affairs is not authorised to give ongoing notices because it is not an interception agency.

This practice was also identified at different agencies during the previous two inspection periods. We provided advice to the effect that a series of historic preservation notices may be interpreted as being akin to an ongoing notice, which only an interception agency may give.

Foreign preservation notice given in an ongoing manner

Our Office identified that the AFP gave five consecutive foreign preservation notices in response to a single request by a foreign country under s 107P of the Act. This section enables foreign countries to request the AFP to arrange for the preservation of stored communications for the purposes of enforcing a foreign law. Such a preservation notice can only be made if the foreign country intends to make an access request under the *Mutual Assistance in Criminal Matters Act 1987*, commonly referred to as a mutual assistance request.

A comparison can be drawn between foreign preservation notices and historic domestic preservation notices as both only require the carrier to preserve stored communications the carrier holds up until the end of the day it receives the notice. The TIA Act does not provide for the extension or renewal of a foreign preservation notice. In our view, the AFP should not give consecutive foreign preservation notices in response to a single request by a foreign country made under s 107P of the TIA Act. This practice, in effect, gives a foreign preservation notice on an ongoing basis, which is not provided for under the TIA Act.

We suggested the AFP seek legal advice on this practice and how it should handle similar requests in the future. The AFP agreed it would obtain legal advice on a case by case basis. We will monitor this issue at future stored communications inspections at the AFP.

Delegation-related non-compliance

The TIA Act provides for the chief officer of a law enforcement agency to authorise or delegate the use of certain powers to specific individuals or classes of individuals within the agency. For example, under s 5AB(1) the chief officer may authorise another person in

writing to be an authorised officer. In turn, under s 107M(2) authorised officers may give ongoing domestic preservation notices. Under s 110(3), the chief officer may authorise persons in writing to apply for stored communications warrants who may, in turn, also give historic domestic preservation notices under s 107M(1).

In assessing whether those persons who have exercised the powers of the chief officer were authorised or delegated to do so, our Office requires agencies to provide copies of their authorisation and delegation instruments relevant to the inspection period.

In 2017–18, we noted an increase in instances where non-compliance occurred as a result of delegation and authorisation issues, the majority of which were disclosed by agencies. This increase is of concern and our Office will monitor agencies’ remedial actions closely.

We suggest agencies remind officers exercising stored communications powers to ensure they are appropriately delegated and/or authorised to do so. Clear and ongoing communication regarding updates, or amendments of delegations and/or authorisations are vital in ensuring officers within agencies are aware of their responsibilities. Effective stored communications training, application checklists that prompt applicants to check for appropriate delegation or authorisation, and strong quality assurance processes also mitigate against non-compliance.

Destruction-related non-compliance

Section 150(1) of the TIA Act states that if the chief officer of an agency is satisfied a record obtained by accessing stored communications is not likely to be required for a permitted purpose, then the chief officer must cause the record to be destroyed forthwith.

The TIA Act does not provide for the chief officer to delegate their obligations under s 150(1). As a result, the chief officer must personally cause each destruction of an agency’s stored communications records. However, obtaining the chief officer’s approval in each instance may be impractical for agencies that hold high volumes of stored communications records. In the absence of an explicit delegation provision, some agencies have relied on the *Carltona* principle to imply that a person in a senior role is authorised to cause the destruction of the records on the chief officer’s behalf.¹³ In these circumstances, we have informed agencies it is better practice for this process to be captured in a written authorisation signed by the chief officer. We note that it is ultimately up to agencies to seek their own advice about whether they may reasonably rely on the *Carltona* principle.

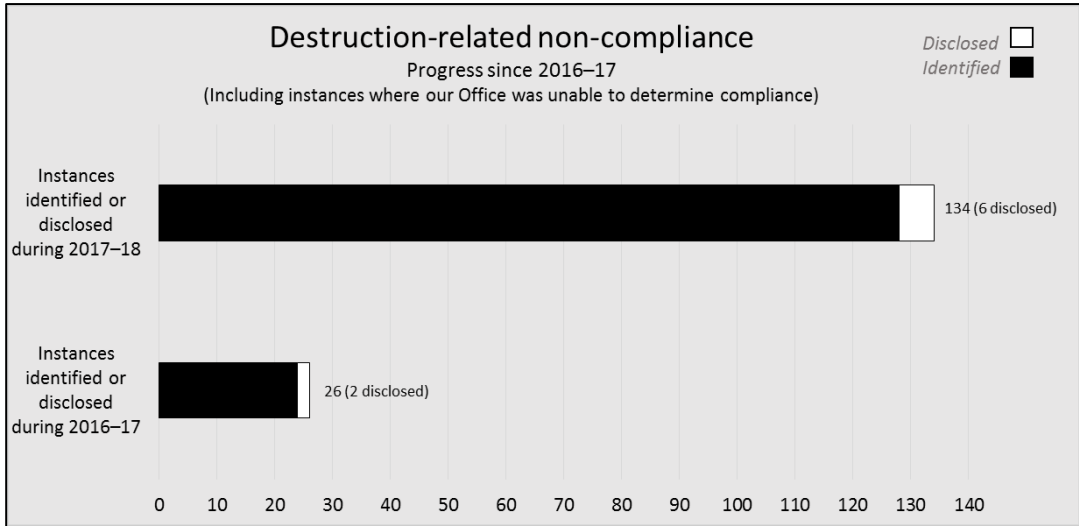
¹³ The *Carltona* principle established in *Carltona v Commissioner of Works* [1943] 2 All ER 560, provides that legislation may allow for an implied authorisation of a person’s functions and powers to be undertaken by another person, as a matter of administrative convenience. The *Carltona* principle is likely to apply in circumstances where: the administrative power is of a more routine nature, the person being authorised is of a high or senior level, and the authorisation is administratively or practically necessary.

‘Forthwith’—being the standard applied to destruction—is not a timeframe defined in the TIA Act or elsewhere. We previously sought advice from the AGD, in its former role as the TIA Act’s administrator, on how the term should be applied when assessing an agency’s compliance. The AGD’s view was that, although forthwith should not be applied as a strict timeframe, the term does indicate a level of urgency. With this in mind, we assess compliance based on what we think is reasonable for each agency, given what we know of its processes.

At eight of the 17 agencies the Office inspected during 2017–18, we identified instances of non-compliance, or instances where we were unable to determine compliance, relating to agencies’ destruction obligations under s 150(1). While the details of each instance differed, all could be broadly grouped under the following categories:

- stored communications records that were destroyed long after being certified for destruction, or records where there was nothing to indicate when destruction had occurred
- copies of stored communications records that had been certified for destruction but were located during an inspection
- stored communications records, including copies, which had been destroyed prior to being certified for destruction.

The number of agencies with instances of destruction-related non-compliance increased during 2017–18. As such, compliance with these requirements continues to be a matter of focus for our Office. We suggest agencies continue to apply targeted training measures to address these issues. We also suggest agencies review the effectiveness of their destruction processes, particularly regarding the timing of destruction of stored communications records. Our Office will continue to monitor these issues at future inspections.



Previous recommendation highlighted to Home Affairs

At our 2015–16 inspection at the former Australian Customs and Border Protection Service, no records were available to demonstrate who within the agency had authorised the destruction of stored communications, or when the approval had been given. As a result, our Office could not determine whether these stored communications had been destroyed in accordance with s 150(1) of the TIA Act. The Ombudsman made a recommendation about this issue.

During 2017–18, we again identified instances of non-compliance with s 150(1). It was unclear to us whether the agency had taken remedial action in response to the 2015–16 recommendation. For two warrants, a record on file indicated that copies of accessed stored communications had been destroyed, however the record did not provide sufficient details to determine whether this destruction occurred in accordance with the requirements of the TIA Act. Based on the records available, we concluded DIBP did not appear to have a formal, consistent approach to destroying stored communications.

As a result of this issue our Office highlighted the previously made recommendation:

Recommendation: *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).*

Our Office will continue to monitor Home Affairs’ remedial action on this issue at future inspections.

Unlawfully accessed stored communications

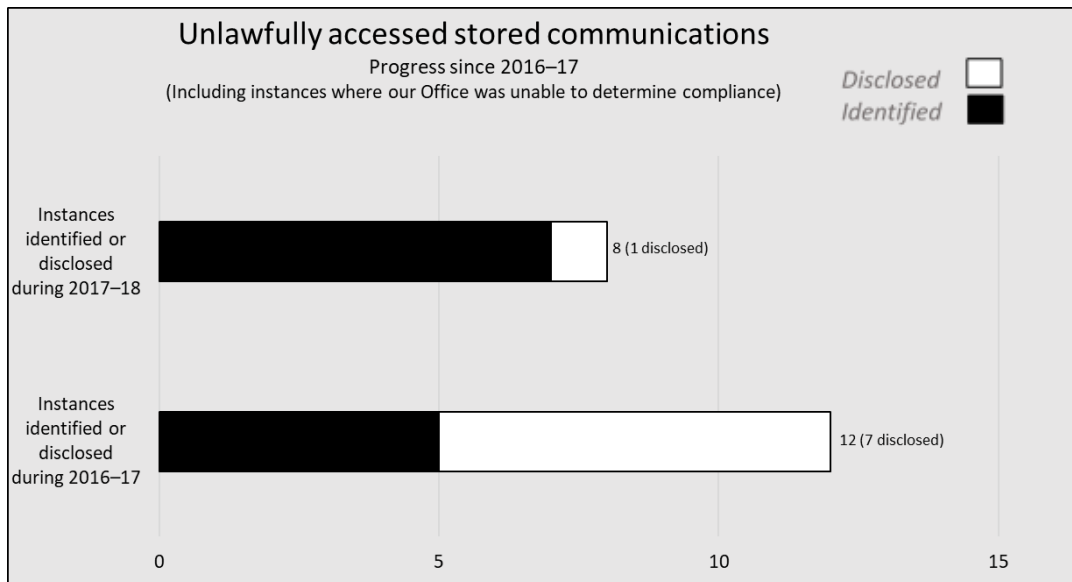
Under s 117 of the TIA Act a stored communications warrant authorises, subject to any conditions or restrictions specified, access to stored communications made by, or sent to, the person listed on the warrant. Section 133 sets out a general prohibition on dealing with accessed information or stored communications warrant information, including information obtained by accessing stored communications in contravention of s 108(1), which prevents access to a stored communication without a warrant.

In 2017–18, three of the 17 agencies we inspected had received stored communications in one of the following two categories:

- the carrier provided insufficient information to determine whether the accessed stored communications related to the person listed on the warrant
- the carrier provided stored communications to the agency which did not comply with conditions and/or restrictions specified on the warrant.

Although these issues relate to carrier errors, in our view it is an agency's responsibility to ensure it is only dealing with lawfully accessed stored communications. In instances where an agency has received unlawfully accessed stored communications from a carrier, our Office reports on the agency's approach to identifying and then quarantining the stored communications from investigators.

We suggest agencies ensure they apply processes to review the lawfulness of stored communications prior to access by investigators. In instances where there is insufficient information to determine the lawfulness of accessed stored communications, we suggest agencies quarantine the stored communications from investigators until their lawfulness can be verified.



Previous recommendation highlighted to Home Affairs

During our inspection in 2015–16, the Australian Customs and Border Protection Service did not provide our Office with copies of accessed stored communications. As such, we were unable to assess whether the stored communications had been lawfully obtained. This resulted in a recommendation being made.

During 2017–18, it appeared DIBP had not fully implemented this recommendation, as it again did not provide us with copies of accessed stored communications obtained under two warrants. In turn, we were unable to determine if DIBP had lawfully accessed stored communications in these instances. DIBP advised that copies of these stored communications were held in regional offices, and were not available during our inspection.

As is required under section 186B(3) of the TIA Act, our Office provides each agency with formal notice of all scheduled inspections. We also send a more detailed notification in the lead-up to an inspection which provides guidance on the type of information the agency should make available during an inspection. We expect each agency to appropriately prepare for our inspections in order to demonstrate their compliance with the TIA Act.

Given the gaps in its records, our Office drew DIBP’s attention to the 2015–16 recommendation:

Recommendation: *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.*

Our Office will continue to monitor Home Affairs' remedial action at future inspections.

Preservation notice left to expire

Section 107L(2)(a)(ii) of the TIA Act states that an issuing agency must revoke a preservation notice if the agency decides not to apply for a warrant under Chapter 3 (or Part 2–5) to access stored communications.

In determining compliance with this provision, our Office assesses, in instances where a preservation notice has expired, if information is available to indicate whether an agency maintained an intention to apply for a stored communications or Part 2–5 warrant. When available records indicate the agency did not maintain an intention to apply for a warrant at the time the preservation notice expired, our Office reports this as non-compliant with s 107L(2)(a)(ii). When no such record is available, we report that we are unable to determine whether the agency complied with s 107L(2)(a)(ii).

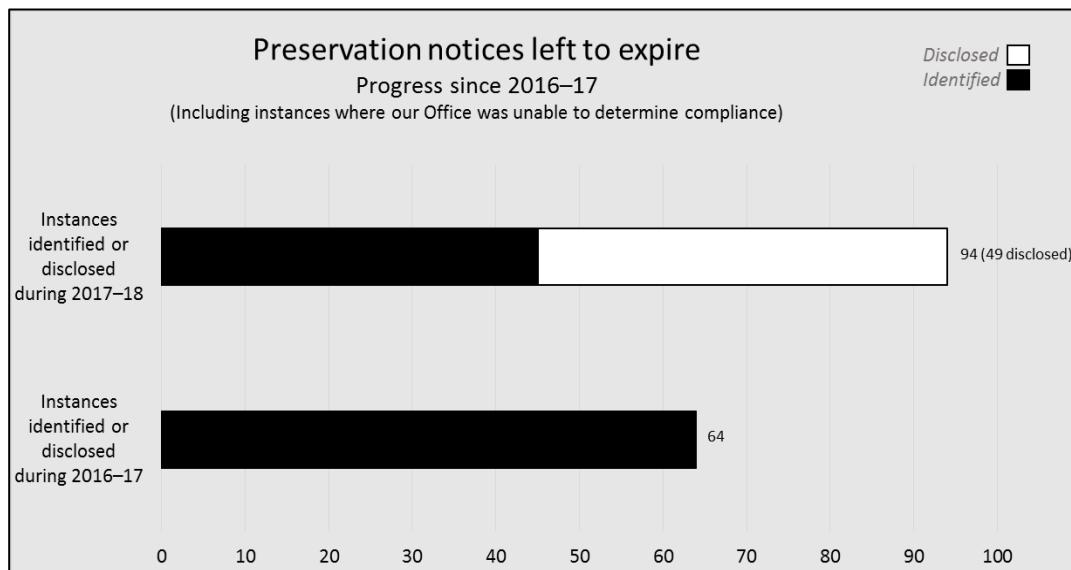
This issue was identified during our inspections in 2016–17. Instances of non-compliance with the mandatory revocation requirements have increased in 2017–18 compared with 2016–17. However, the increase could be a result of agencies more actively disclosing when this occurs, as the number of instances our Office identified has reduced. Our Office sees this increase in the number of disclosures as a demonstration that agencies are becoming more aware of the mandatory revocation requirements.

All agencies we inspected had processes in place to contact investigators to determine whether they still maintained an intention to obtain a warrant. Notwithstanding these processes, in many instances investigators did not respond.

It is clear agencies have attempted to implement solutions to this recurring issue. In our view the person best placed to make a decision on whether a preservation notice should be revoked is usually the investigator. We encourage agencies to continue with awareness raising activities, to remind investigators of the mandatory revocation requirements of the TIA Act.

Our Office also identified five foreign preservation notices at the AFP that were left to expire. Under section 107R of the TIA Act, if a mutual assistance request is not made to the Attorney-General within 180 days from the day the foreign preservation notice is given, the AFP is required to revoke the notice within three working days. In these five instances, as there was nothing to indicate that the Attorney-General had received a mutual assistance

request following the period of 180 days, the AFP was required to revoke the foreign preservation notices.



Record-keeping and reporting issues

Under the TIA Act, agencies have a number of record-keeping obligations against which we assess compliance. Agencies use different methods to satisfy these obligations, including spreadsheets and databases. In some instances the absence of adequate record-keeping processes poses a risk to agencies in assuring the accuracy of their record-keeping and reporting. It also impacts on our Office’s ability to effectively conduct inspections.

During 2017-18 we identified a small number of agencies that had discrepancies in their reports to the Minister. This generally occurred because established processes and procedures were applied inconsistently.

Previous recommendation highlighted to Home Affairs

Following our 2015-16 inspection we made a recommendation to the Australian Customs and Border Protection Service about its record-keeping processes. In its response, the agency advised it had implemented a centralised record-keeping system for all stored communications warrants and preservation notices. At our 2016-17 inspection, it was again apparent the DIBP did not have a centralised record-keeping system and, therefore, the risks previously identified had not been addressed. Following the 2016-17 inspection, the DIBP advised it would implement a manual process to track its stored communications records.

At our most recent inspection in 2017–18, we again identified issues with the DIBP’s record-keeping procedures. For example, DIBP initially advised our Office it had been issued 12 stored communication warrants during the period but we identified that, because a reference number was used twice, the number of stored communication warrants issued was, in fact, 13. In another example, the same reference number was used to identify three separate preservation notices.

Whilst the DIBP advised that it no longer uses the same reference number for multiple records, our Office suggested the DIBP should confirm that it had accurately reported to the Minister.

When discussing this issue, our Office drew the DIBP’s attention to this previous recommendation:

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

In response to our 2017–18 inspection, Home Affairs advised it is actively reviewing how it can best use its existing record management systems to ensure information is recorded effectively. It has also established an internal working group to guide this process and develop appropriate supporting policy documents and training.

Our Office will continue to monitor Home Affairs’ remedial action at future inspections.

Stored communications: good practices

During our inspections we examine the adequacy of agencies’ policies and procedures to ensure compliance with the TIA Act, based on information provided by the agency. This includes identifying practices that assist agencies in achieving compliance, as well as practices that pose risks to agency compliance. Examples of good practices identified during our inspections in 2017–18 are outlined below.

Good practices: agency response to unlawfully received stored communications

Across several agencies, we identified good screening and quarantining processes aimed at ensuring agencies were only dealing with lawfully accessed stored communications.

During 2017–18 we noted a number of instances where these processes were of clear benefit. In two instances at the AFP, it received stored communications that did not relate to the stored communications warrant. In both instances, the AFP immediately identified the issue and quarantined the communications before use or communication could occur.

Good practices: agency processes to address mandatory revocation requirements for preservation notices

Across agencies, we identified good processes for ensuring that preservation notices were revoked in accordance with the requirements of s 107L(2)(a)(ii). These processes typically consisted of compliance areas sending regular reminder emails to investigators throughout the period the preservation notice was in force, to determine whether a stored communications warrant was still required.

We particularly note NSW Police's proactive efforts to ensure compliance with the mandatory revocation requirements. NSW Police is consistently the largest user of the stored communications powers; in 2017–18, it reported to our Office that it gave a total of 359 domestic preservation notices. At the inspection, we identified only 11 preservation notices (3 per cent) that had been left to expire where there were no records to indicate that NSW Police still maintained an intention to obtain a warrant. In all other instances, preservation notices were revoked or there were records on file to indicate that the investigator did maintain an intention to obtain a warrant at the time the notice expired. We also noted records indicating that investigators typically responded to reminder emails. In our view, this indicates NSW Police's processes are working effectively to ensure compliance with s 107L(2)(a)(ii).

Agency findings for 2017–18

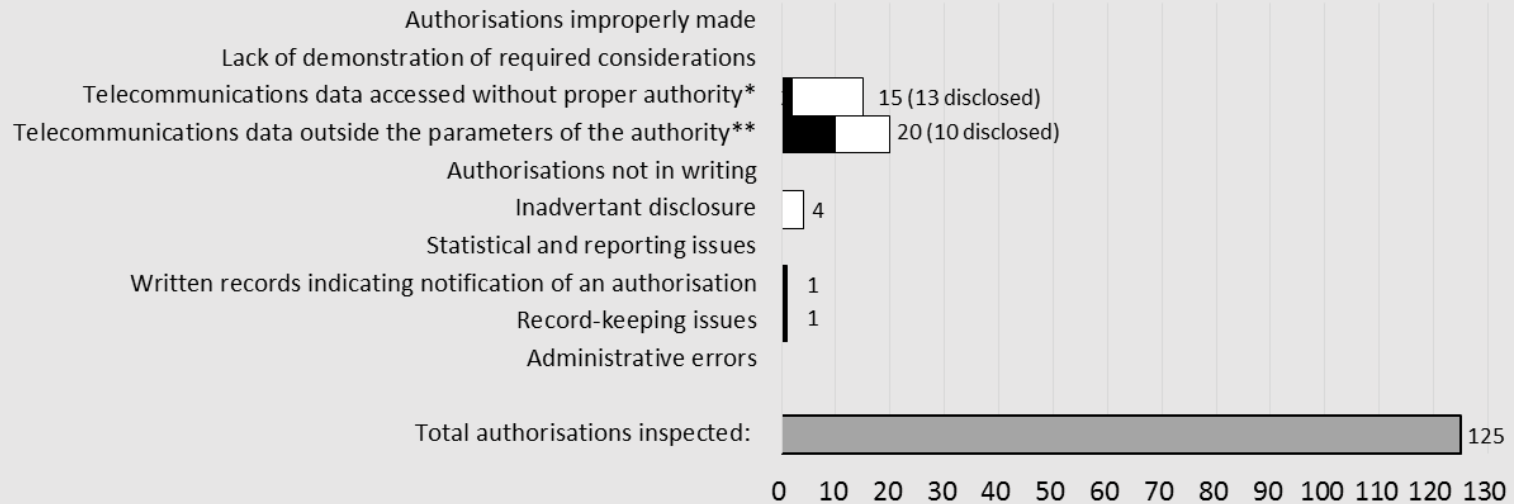
Telecommunications data findings

Australian Criminal Intelligence Commission

Disclosed
Identified



Instances disclosed or identified during 2017–18



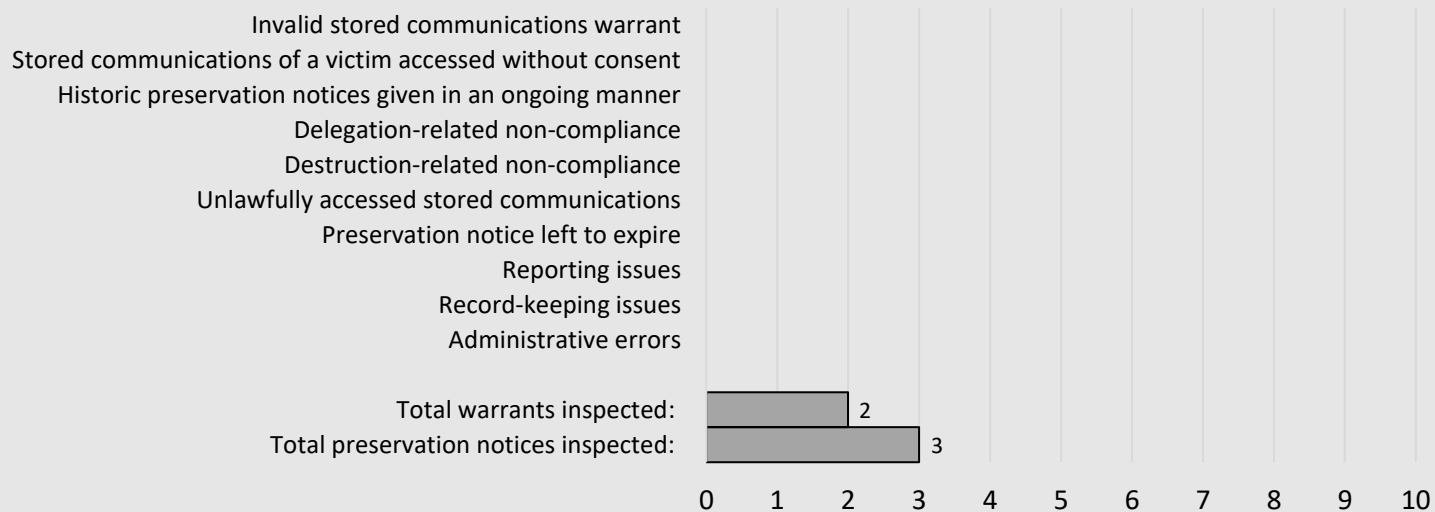
*Where telecommunications data accessed without proper authority, the ACIC notified the carrier of an authorisation prior to it being formally signed by an authorised officer. The ACIC quarantined the telecommunications data obtained in each instance.

**In 15 instances of telecommunications data outside the parameters of the authority, the ACIC continued to receive telecommunications data after a revocation had taken effect. The ACIC has since updated its processes to mitigate reoccurrence of this issue.

Stored communications findings

Australian Criminal Intelligence Commission

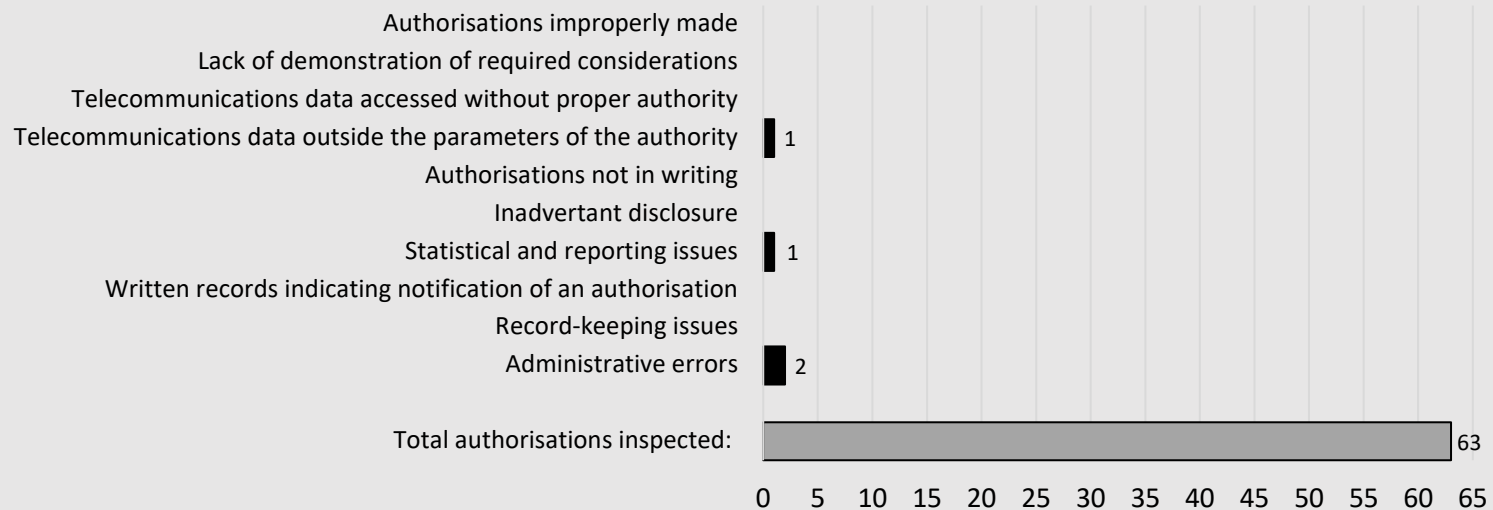
Nil instances of non-compliance identified or disclosed during 2017–18



Telecommunications data findings

Australian Competition and Consumer Commission

Instances identified during 2017–18



Stored communications findings

Australian Competition and Consumer Commission

Powers not used during relevant period - no inspection during 2017–18

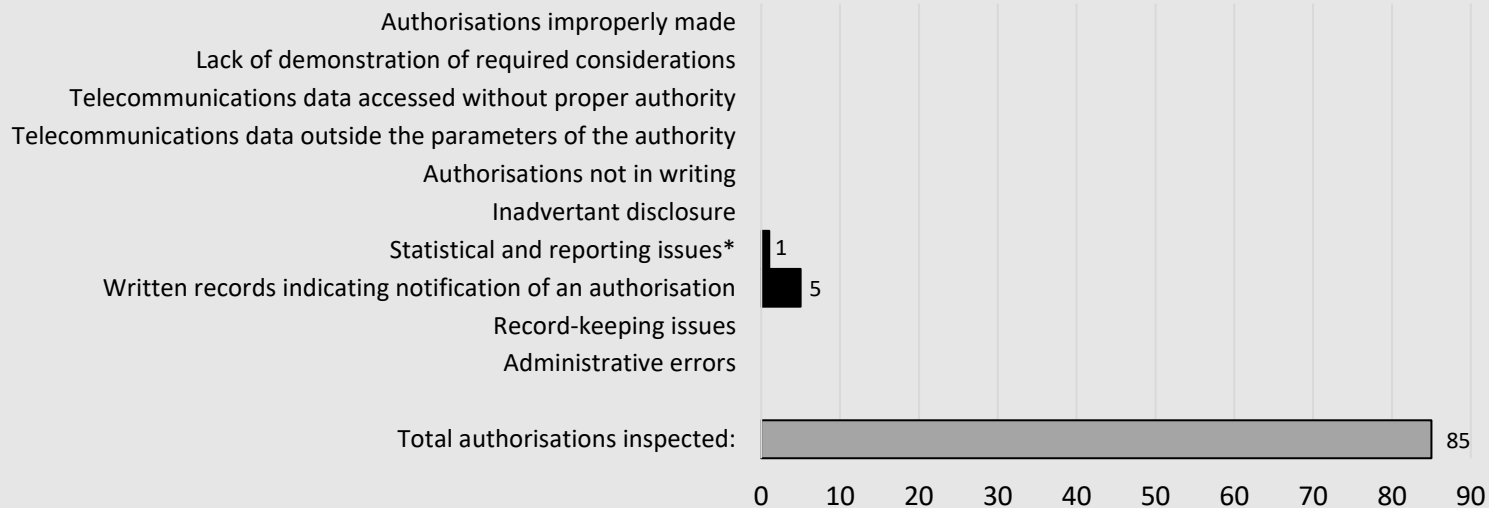
- Invalid stored communications warrant
- Stored communications of a victim accessed without consent
- Historic preservation notices given in an ongoing manner
 - Delegation-related non-compliance
 - Destruction-related non-compliance
- Unlawfully accessed stored communications
 - Preservation notice left to expire
 - Reporting issues
 - Record-keeping issues
 - Administrative errors

No inspection conducted during 2017–18

Telecommunications data findings

Australian Commission for Law Enforcement Integrity

Instances identified during 2017–18



*Regarding the statistical and reporting issue, prior to the inspection, our Office requested statistical data from ACLEI and based on this data there appeared to be an inconsistency between the numbers of authorisations made as provided to our Office compared to those reported to the Minister. ACLEI advised that this inconsistency was due to the method in which the statistics were compiled. In response to this issue ACLEI advised that, in future, a consistent method will be used.

Stored communications findings

Australian Commission for Law Enforcement Integrity

Powers not used during relevant period - no inspection during 2017–18

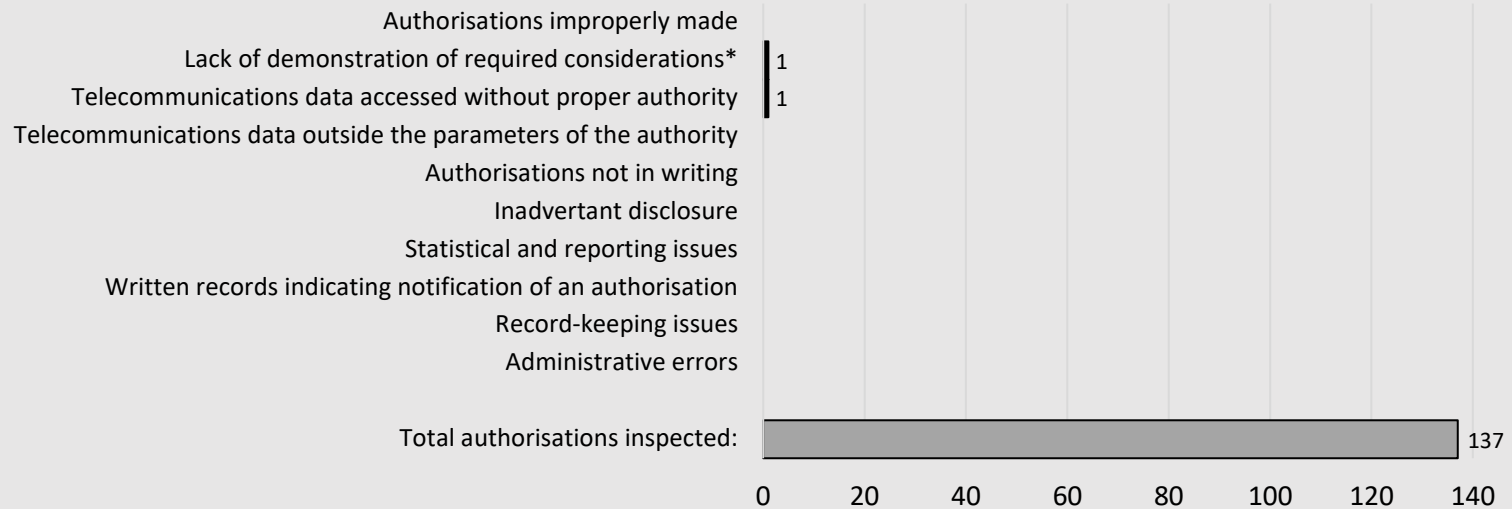
- Invalid stored communications warrant
- Stored communications of a victim accessed without consent
- Historic preservation notices given in an ongoing manner
 - Delegation-related non-compliance
 - Destruction-related non-compliance
- Unlawfully accessed stored communications
 - Preservation notice left to expire
 - Reporting issues
 - Record-keeping issues
 - Administrative errors

No inspection conducted during 2017–18

Telecommunications data findings

Australian Federal Police

Instances identified during 2017–18

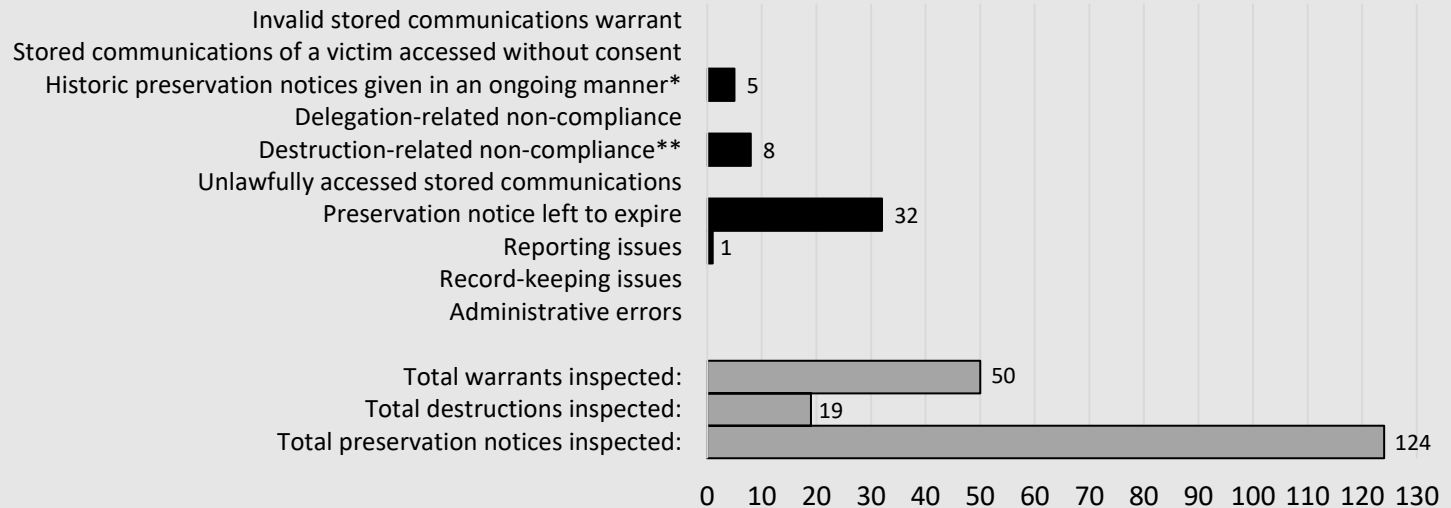


*Regarding instance relating to lack of demonstration of required considerations, recommendation made to the AFP as detailed on page 17.

Stored communications findings

Australian Federal Police

Instances identified during 2017–18



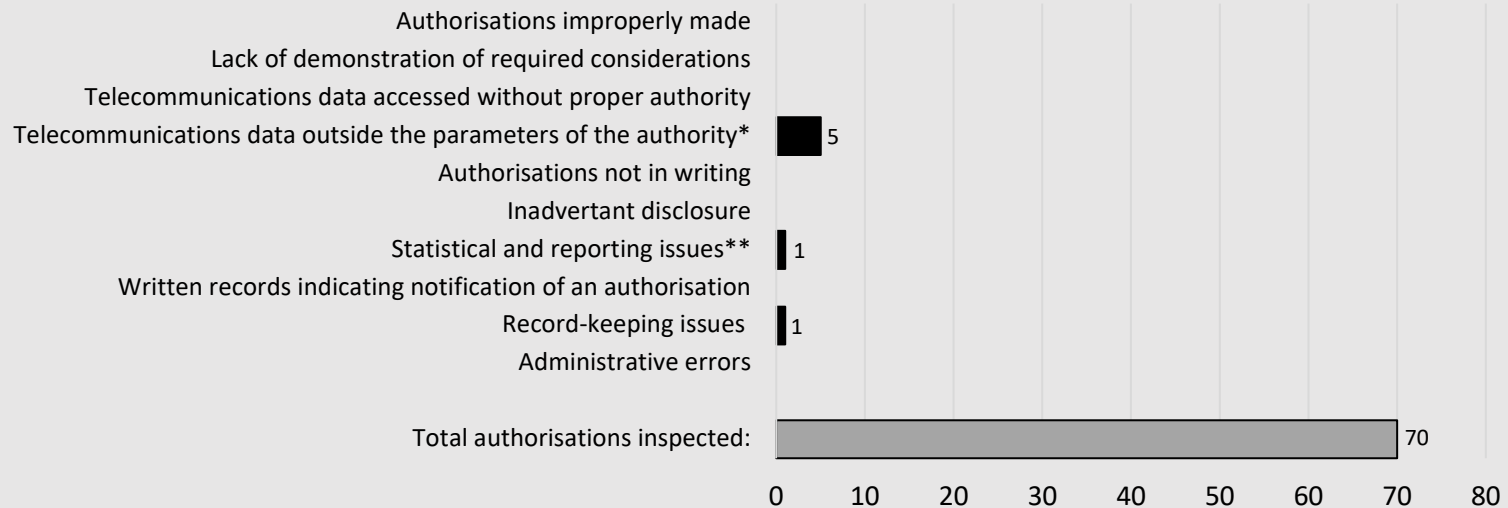
*Instances of historic preservation notices given in an ongoing manner are discussed at pages 34 and 35 of this report.

**During our inspection it appeared that, in seven instances of destruction-related non-compliance, stored communications were destroyed more than two weeks after being certified for destruction. Following the inspection, the AFP advised that the stored communications in these instances had been destroyed at the time they were certified for destruction and the misunderstanding was a result of ambiguous wording used on destruction records which were presented to our Office during the inspection. The AFP has since amended this wording to reduce ambiguity.

Telecommunications data findings

Australian Securities and Investments Commission

Instances identified during 2017–18



*In one instance where telecommunications data outside the parameters of the authority, our Office was unable to determine whether the telecommunications data received from the carrier was within the parameters of the authority because the carrier had not specified the telecommunications service to which the information related.

**Regarding instance of statistical and reporting issues, due to the way in which ASIC had interpreted the reporting requirements to the Minister, a small subset of authorisations made may have been inconsistently reported. ASIC has since updated its processes to ensure accurate reporting to the Minister.

Stored communications findings

Australian Securities and Investments Commission

Powers not used during relevant period - no inspection during 2017–18

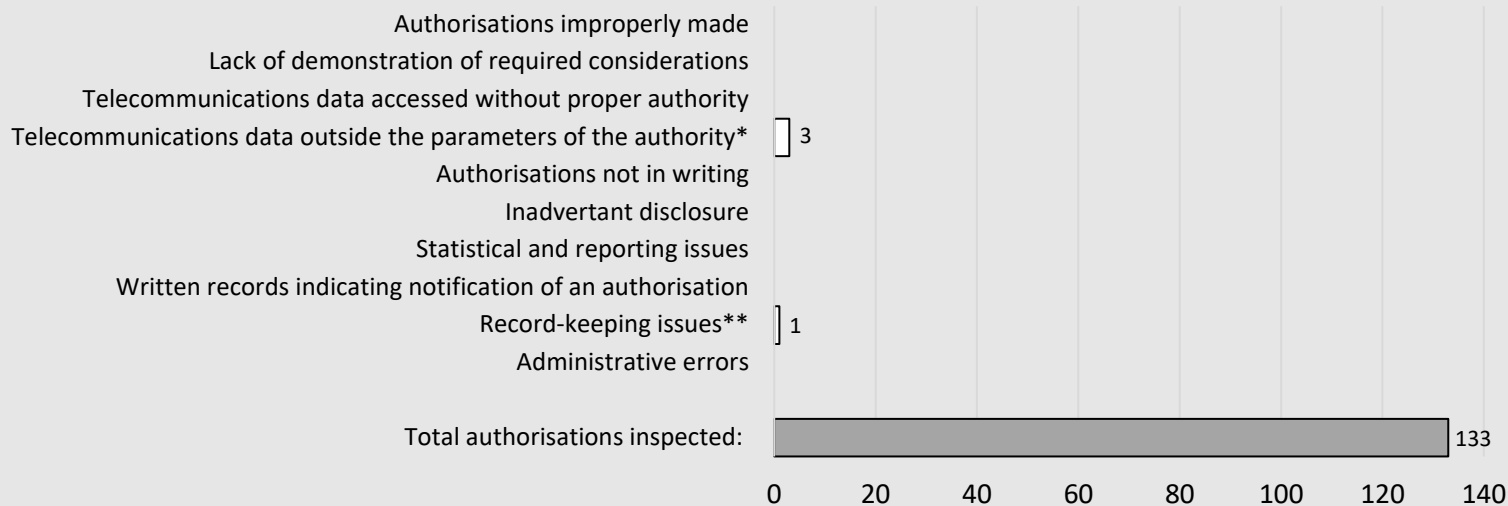
- Invalid stored communications warrant
- Stored communications of a victim accessed without consent
 - Historic preservation notices given in an ongoing manner
 - Delegation-related non-compliance
 - Destruction-related non-compliance
 - Unlawfully accessed stored communications
 - Preservation notice left to expire
 - Reporting issues
 - Record-keeping issues
 - Administrative errors

No inspection conducted during 2017–18

Telecommunications data findings

Corruption and Crime Commission (Western Australia)

Instances disclosed during 2017–18



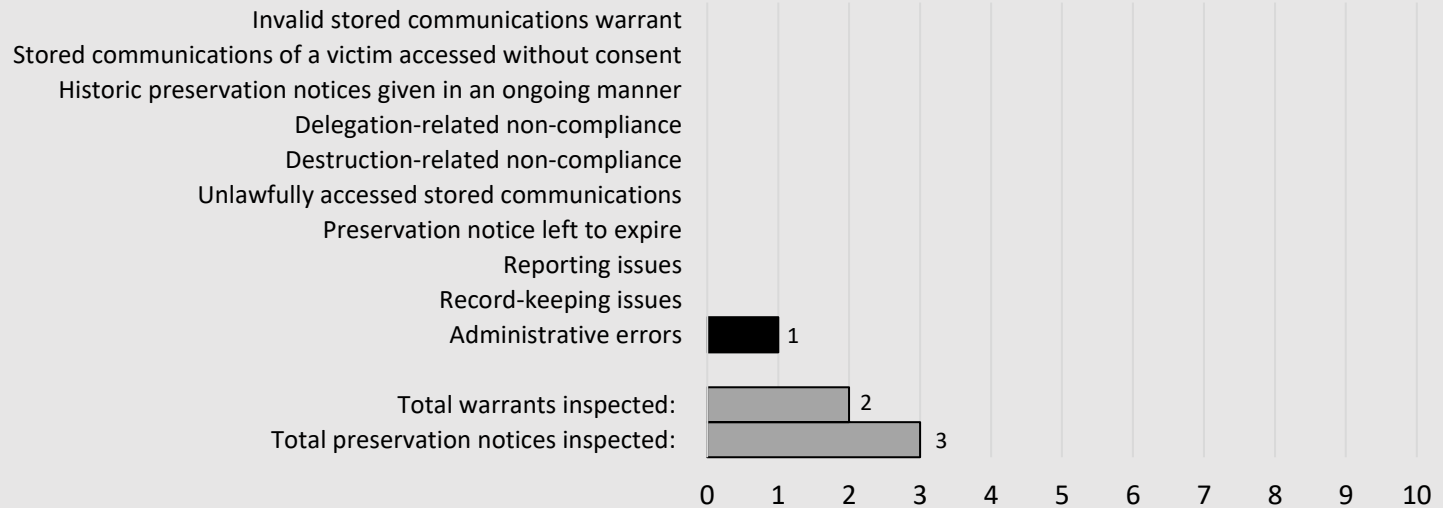
*In one instance of telecommunications data outside the parameters of the authority, the CCC (WA) was unable to locate the authorisation for access to telecommunications data. As a result, our Office was unable to assess whether the results obtained in relation to this authorisation were within the parameters specified on the authority.

**As discussed above, in one instance relating to record-keeping issues the CCC (WA) was unable to locate an authorisation. In this instance, our Office relied on the CCC (WA)'s processes and procedures to confirm the access to telecommunications data had been appropriately authorised.

Stored communications findings

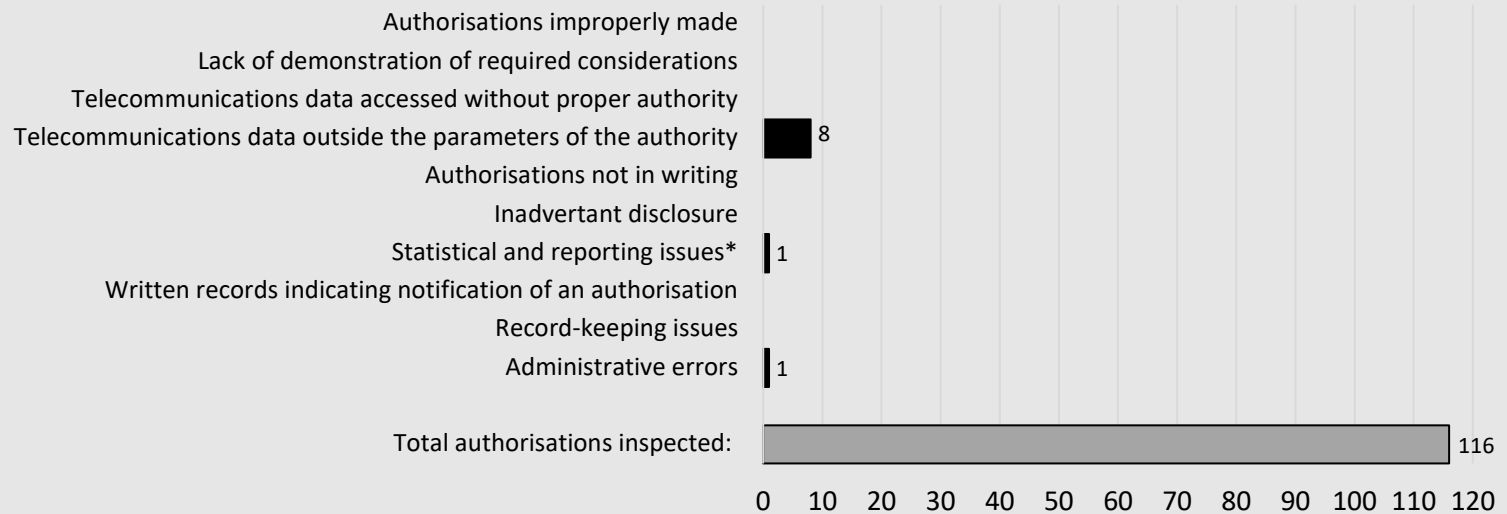
Corruption and Crime Commission (Western Australia)

Instances identified during 2017–18



Telecommunications data findings Crime and Corruption Commission (Queensland)

Instances identified during 2017–18

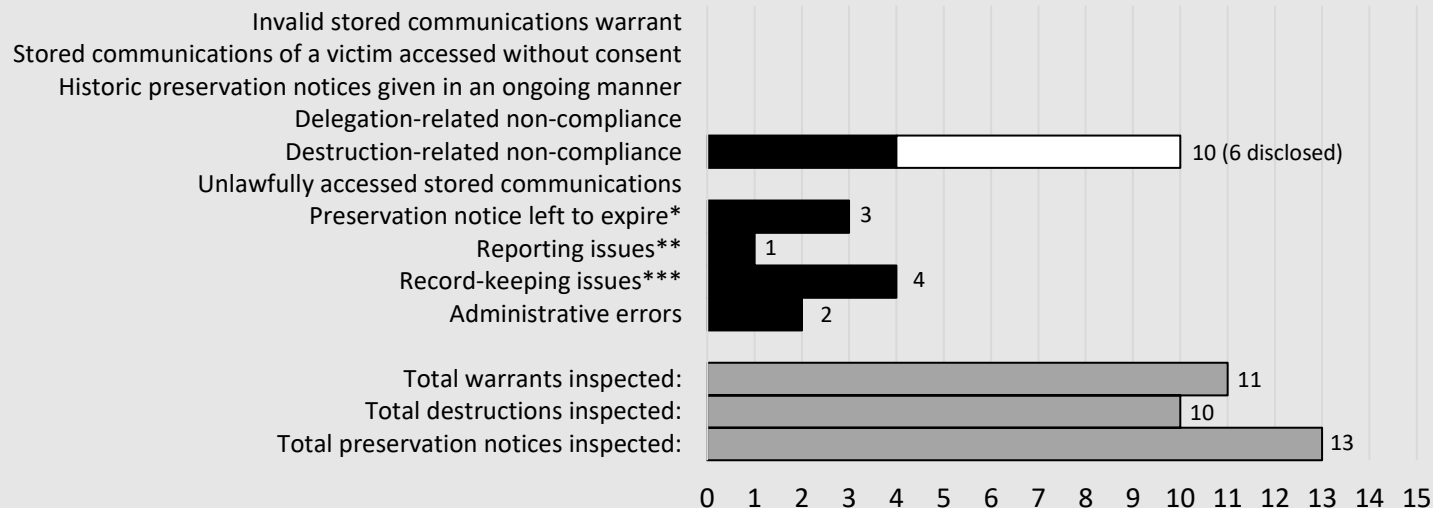


*Regarding statistical and reporting issues - during our previous inspection in 2016–17, we identified inconsistencies in how authorisations were being reported to our Office and to the Minister. This issue was again identified during 2017–18, however our Office noted improvements in the way in which the CCC (QLD) were compiling its statistics for reporting purposes. Furthermore, the CCC (QLD) has implemented a number of remedial actions to reduce inconsistencies including quarterly reviews of authorisations made. Our Office will continue to monitor the CCC (QLD)'s progress in relation to this issue.

Stored communications findings Crime and Corruption Commission (Queensland)

Disclosed
Identified

Instances disclosed or identified during 2017–18



*We acknowledge that instances of preservation notices left to expire occurred prior to the CCC (QLD)'s implementation of amended revocation processes.

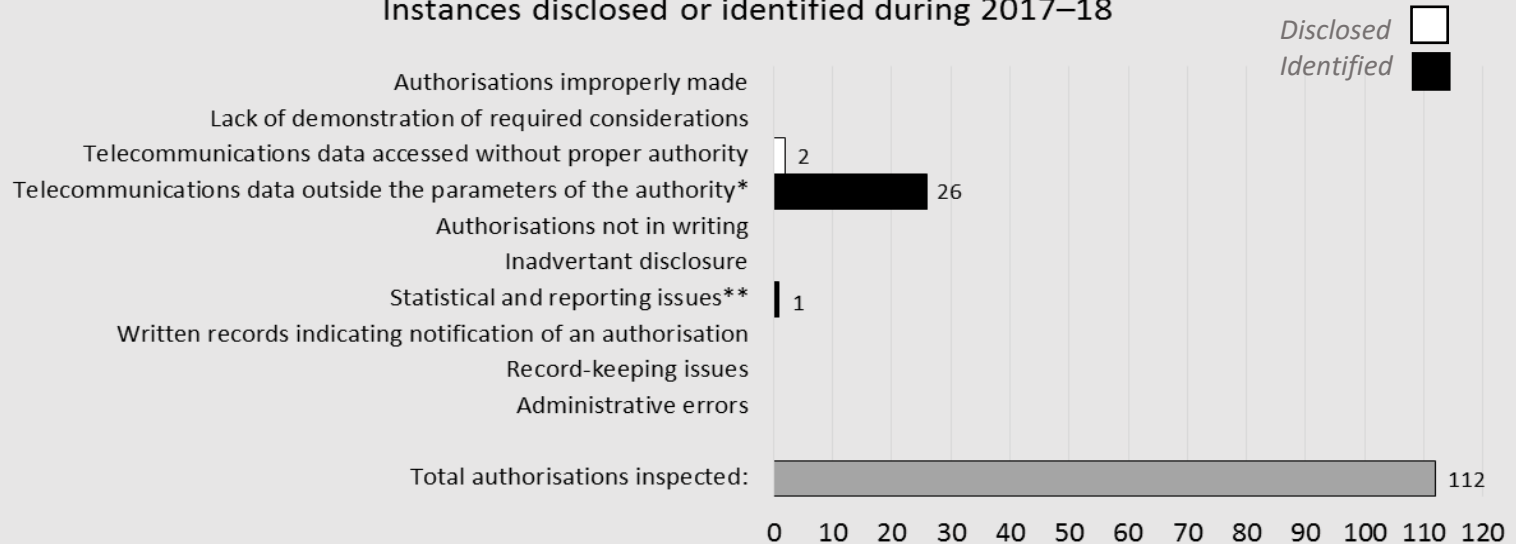
**Regarding reporting issues - following the inspection, the CCC (QLD) advised that an addendum report, addressing the discrepancies in calculations, has been included in the 2017–18 annual report and provided to the Minister.

***Regarding record-keeping issues - our Office identified four instances where the CCC (QLD) had not retained a complete copy of a preservation notice given.

Telecommunications data findings

Former Department of Immigration and Border Protection

Instances disclosed or identified during 2017–18





*25 instances where telecommunications data outside the parameters of the authority were the result of automatic, and unintentional, input from DIBP’s electronic database. In response to this issue being identified in 2016–17, Home Affairs updated its processes to mitigate recurrence of this issue. However, this process was only adopted for prospective authorisations. During this inspection we suggested that Home Affairs consistently apply this process to historic authorisations.

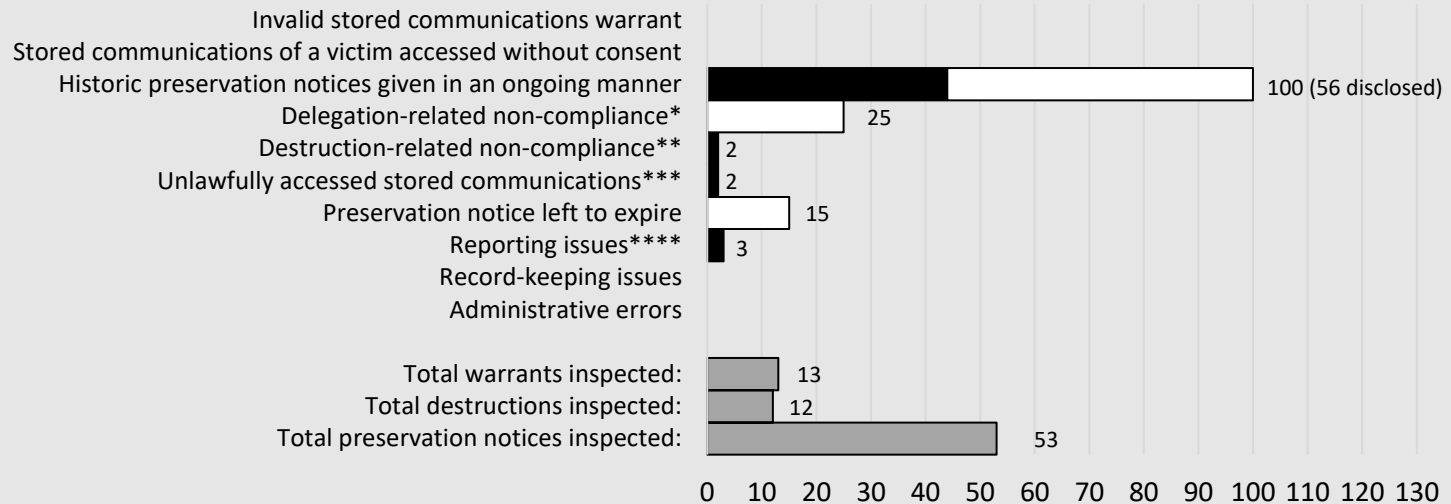
** Regarding statistical and reporting issues - during our previous inspection, we identified inconsistencies in how authorisations were being captured in Home Affairs’ electronic database. This issue was again identified during 2017–18. Home Affairs advised that, for the purpose of reporting to the Minister, it had manually captured the number of authorisations made. Based on our understanding of this process, we are satisfied that the reporting obligations to the Minister have been met and are accurate.

Stored communications findings

Former Department of Immigration and Border Protection

Instances disclosed or identified during 2017–18

Disclosed 
 Identified 

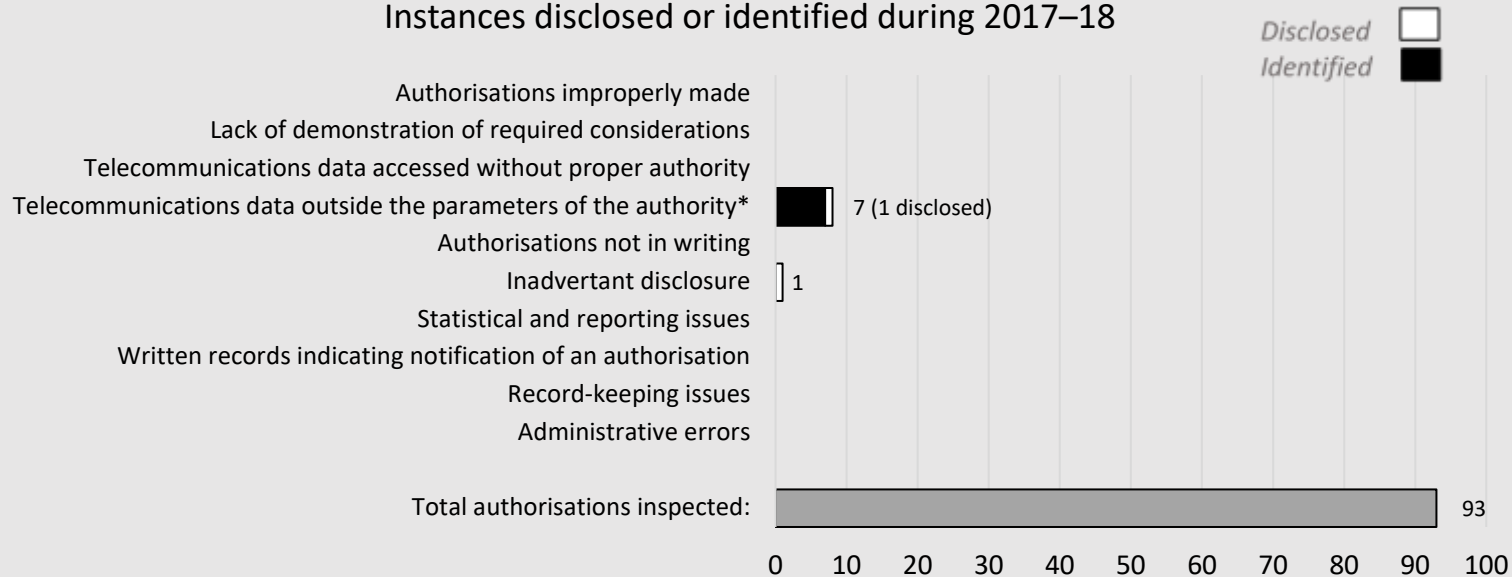


*Delegation-related non-compliance discussed at page 35 of this report.
 **Destruction-related non-compliance discussed at page 36 of this report.
 ***Unlawfully accessed stored communications discussed at page 39 of this report.
 ****Instances of reporting issues discussed at page 42 of this report.

Telecommunications data findings

Independent Broad-based Anti-corruption Commission

Instances disclosed or identified during 2017–18

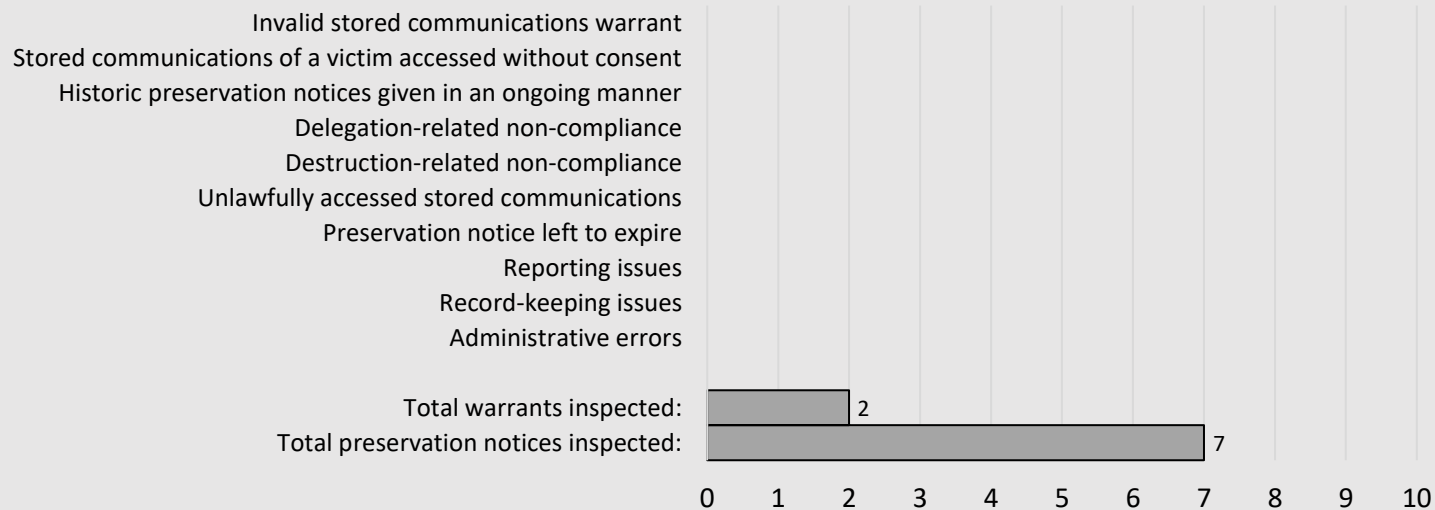


*Our Office acknowledges that six instances of telecommunications data outside the parameters of the authority were not initially addressed by IBAC as a result of IBAC receiving incomplete advice from our Office at the previous inspection in 2016–17. This advice was clarified with IBAC in February 2018 and IBAC amended its processes to mitigate reoccurrence.

Stored communications findings

Independent Broad-based Anti-corruption Commission

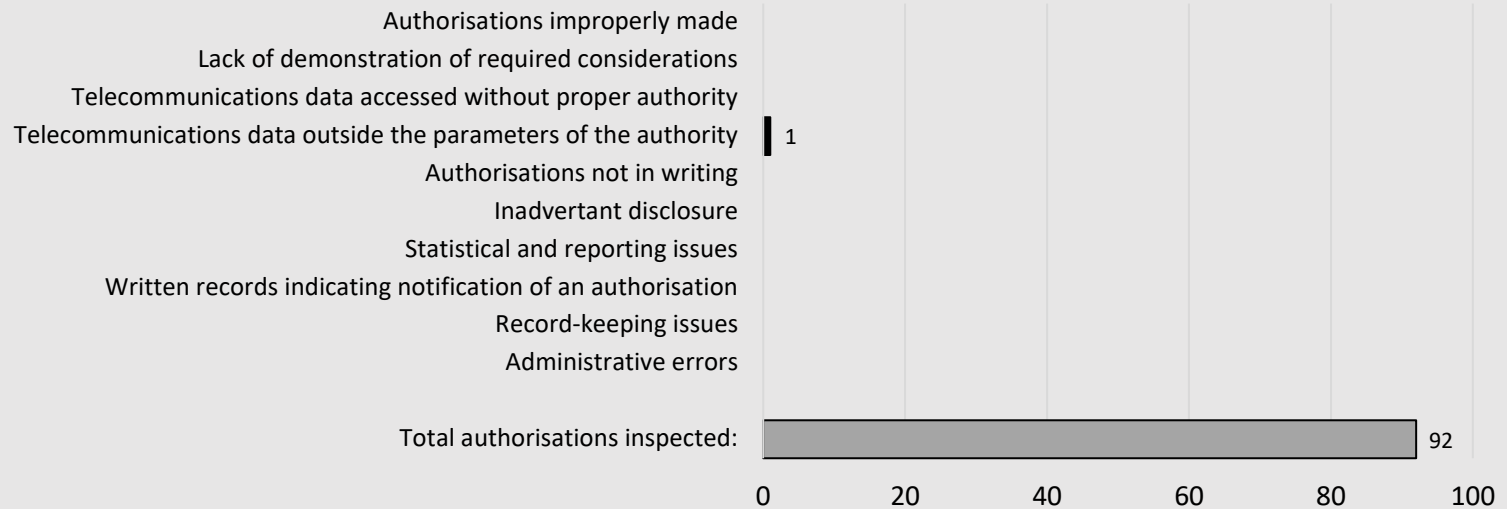
Nil instances of non-compliance identified or disclosed during 2017–18



Telecommunications data findings

Former Police Integrity Commission

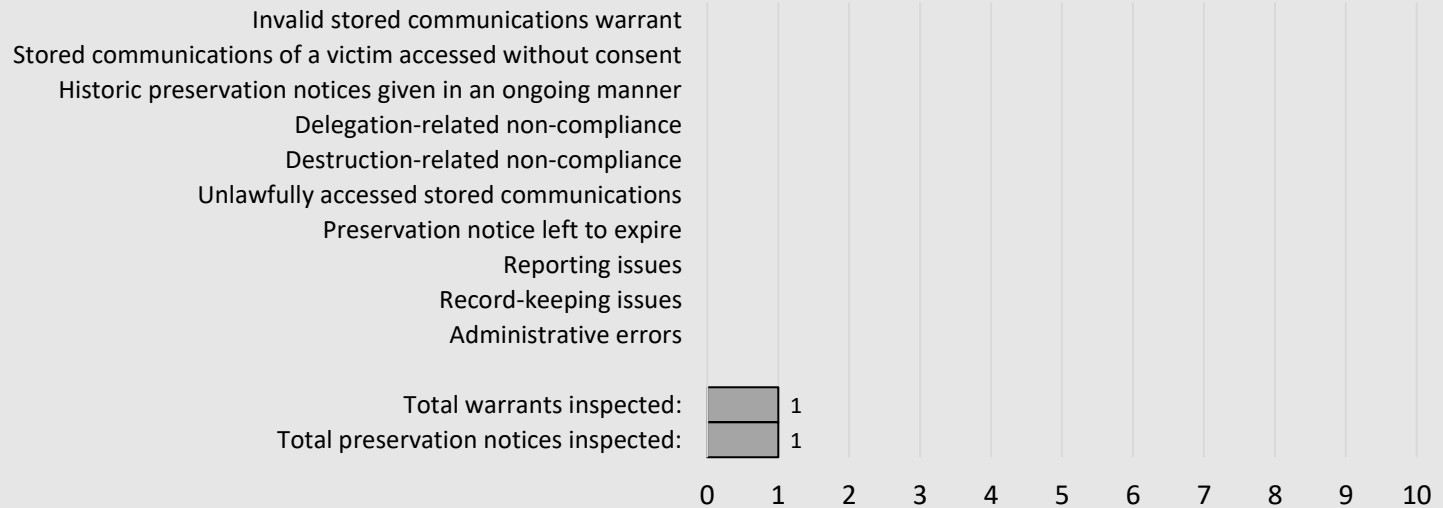
Instances identified during 2017–18



Stored communications findings

Former Police Integrity Commission

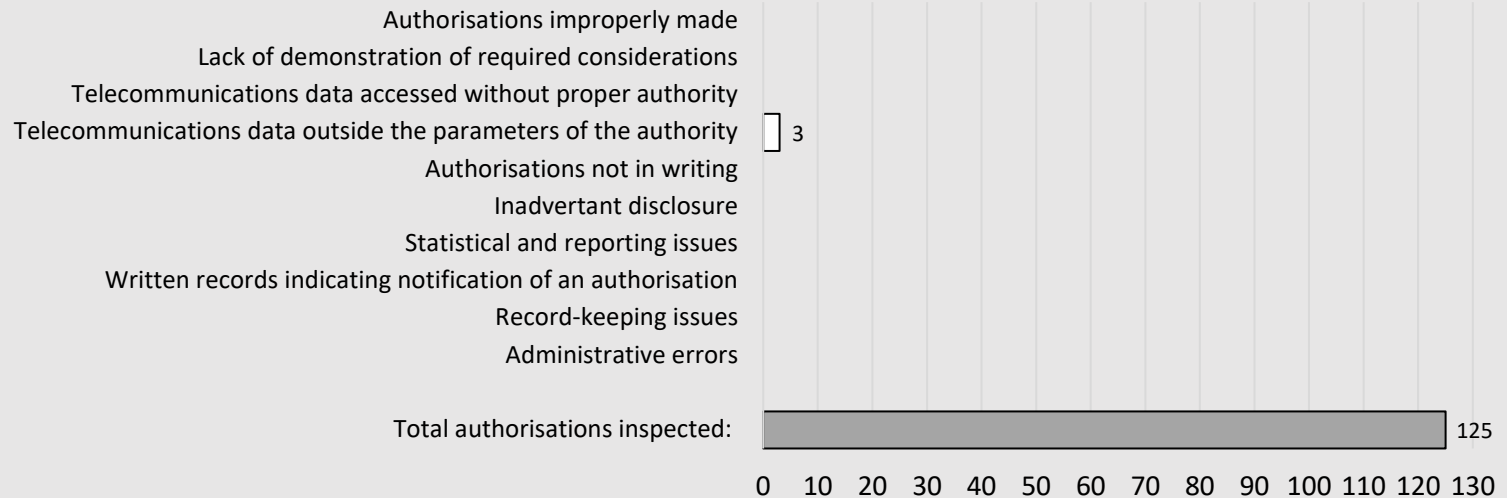
Nil instances of non-compliance identified or disclosed during 2017–18



Telecommunications data findings

New South Wales Crime Commission

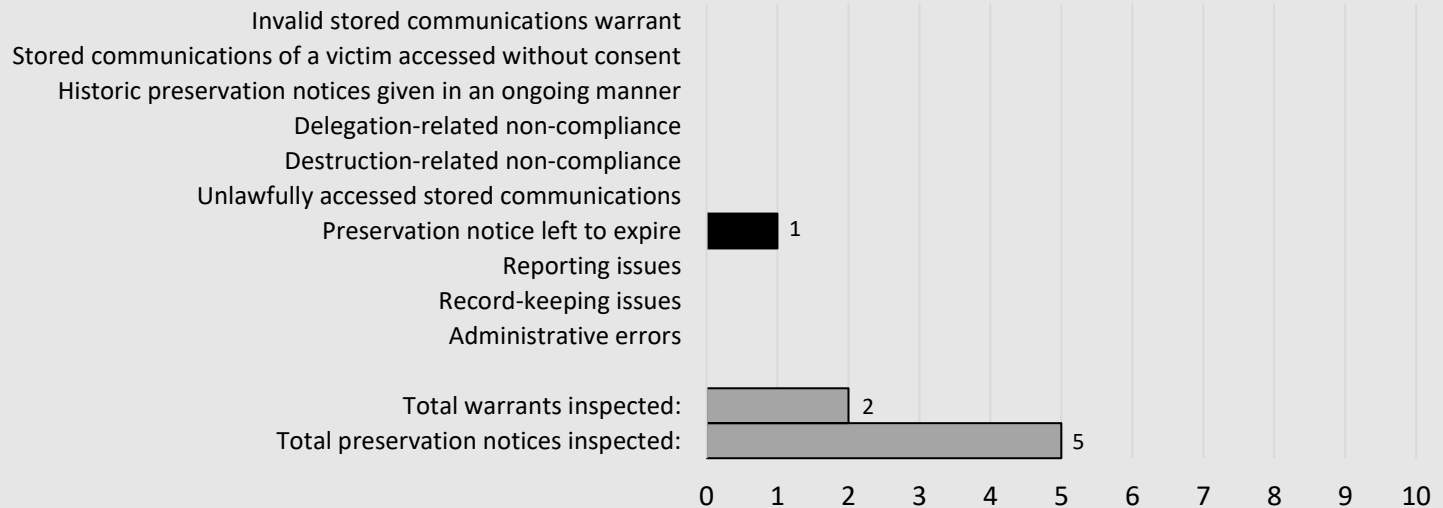
Instances disclosed during 2017–18



Stored communications findings

New South Wales Crime Commission

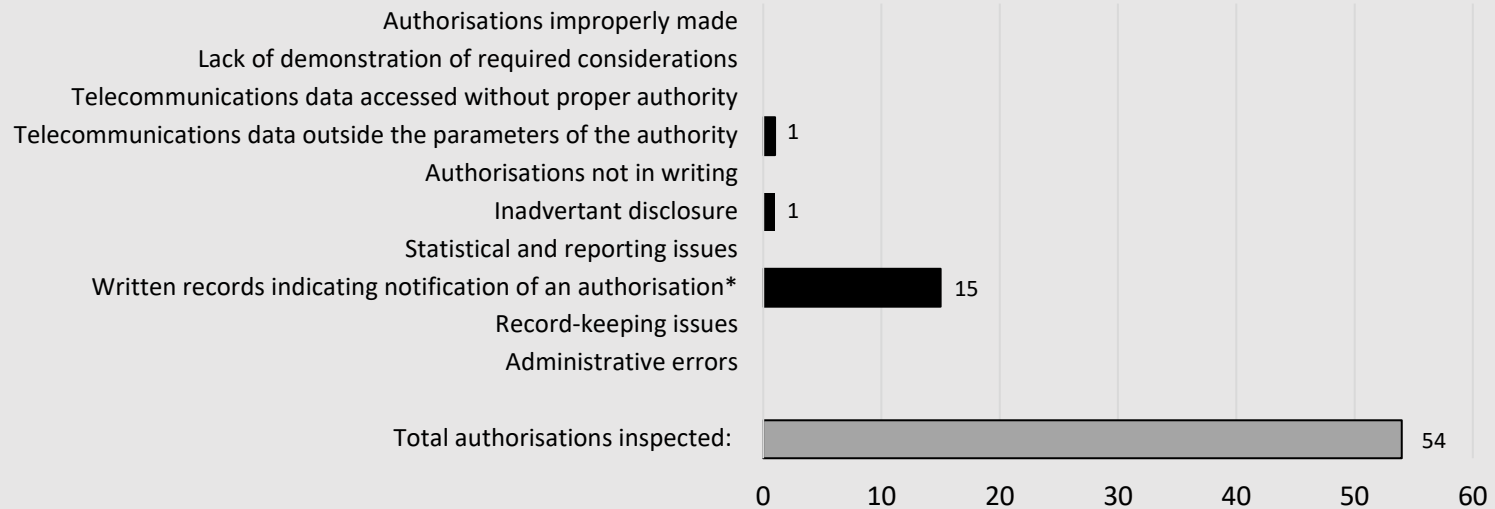
Instances identified during 2017–18



Telecommunications data findings

Independent Commission Against Corruption (New South Wales)

Instances identified during 2017–18

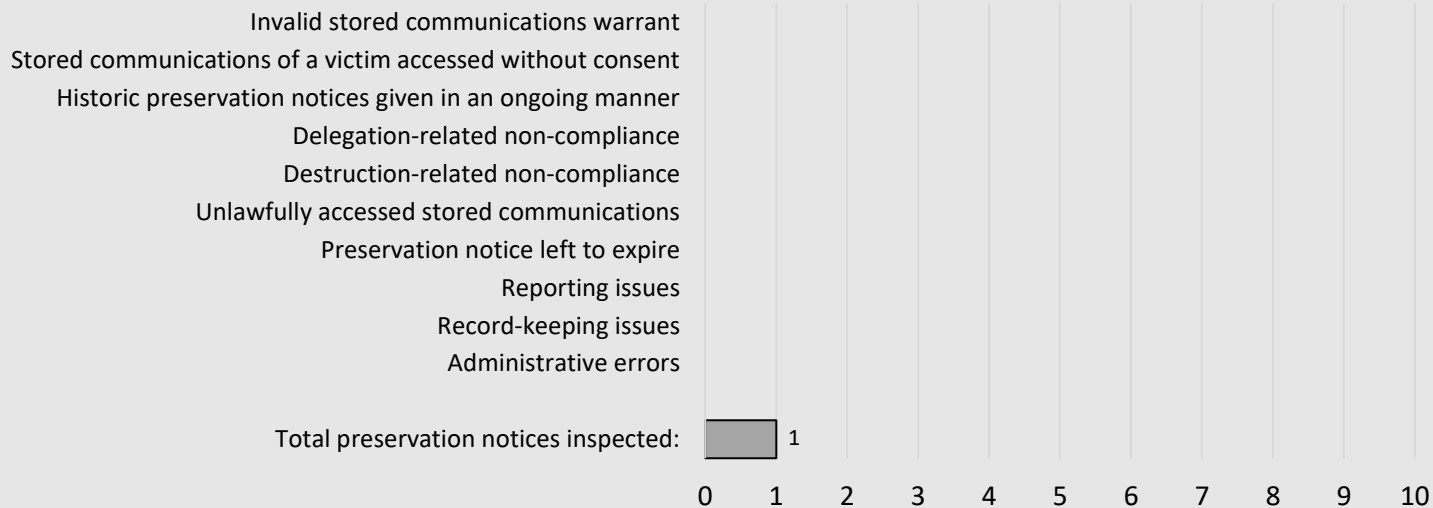


*Instances of non-compliance regarding written records indicating notification of an authorisation were also identified during 2016–17, however each instance occurred prior to ICAC (NSW) receiving the findings from that inspection.

Stored communications findings

Independent Commission Against Corruption (New South Wales)

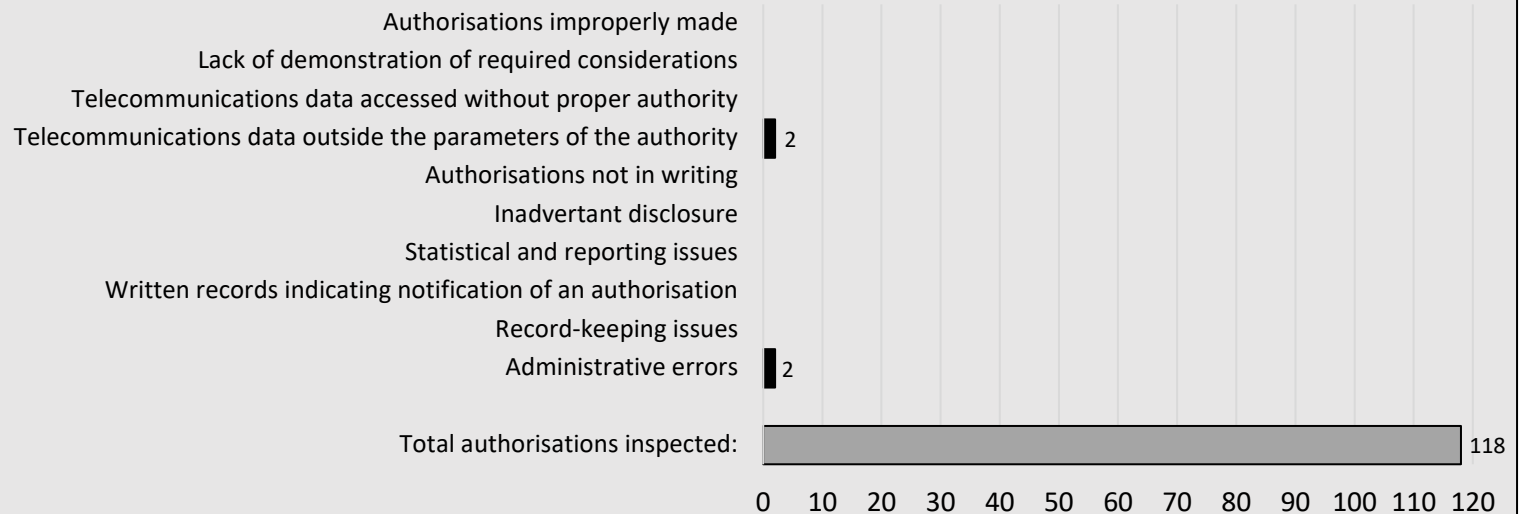
Nil instances of non-compliance identified or disclosed during 2017–18



Telecommunications data findings

New South Wales Police Force

Instances identified during 2017–18

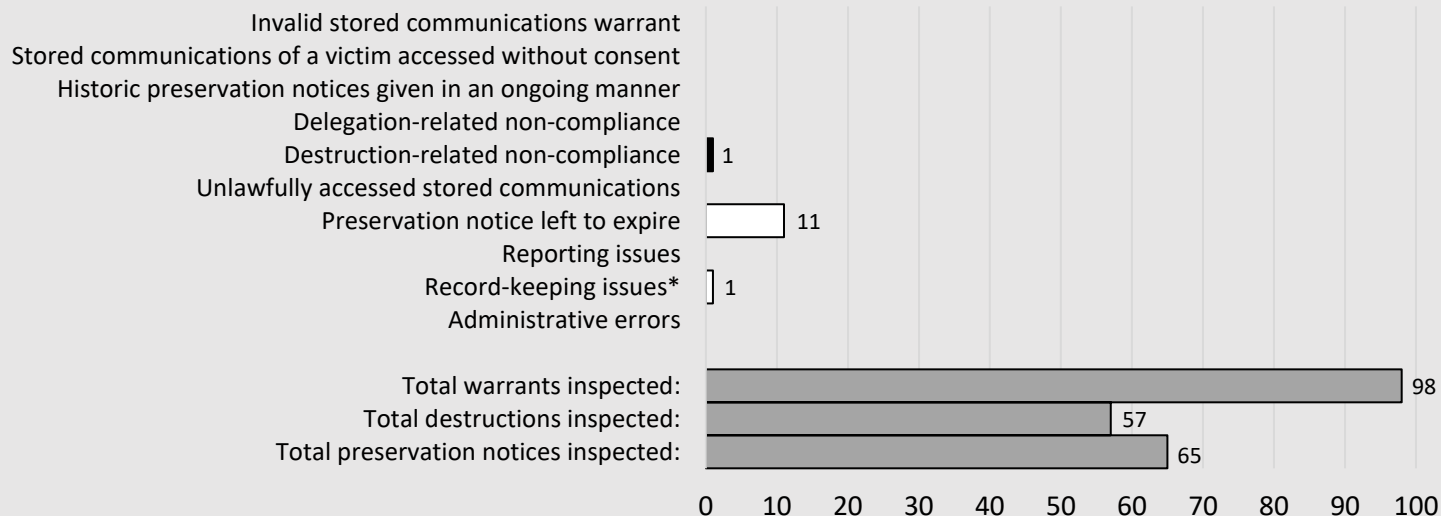


Stored communications findings

New South Wales Police Force

Instances disclosed or identified during 2017–18

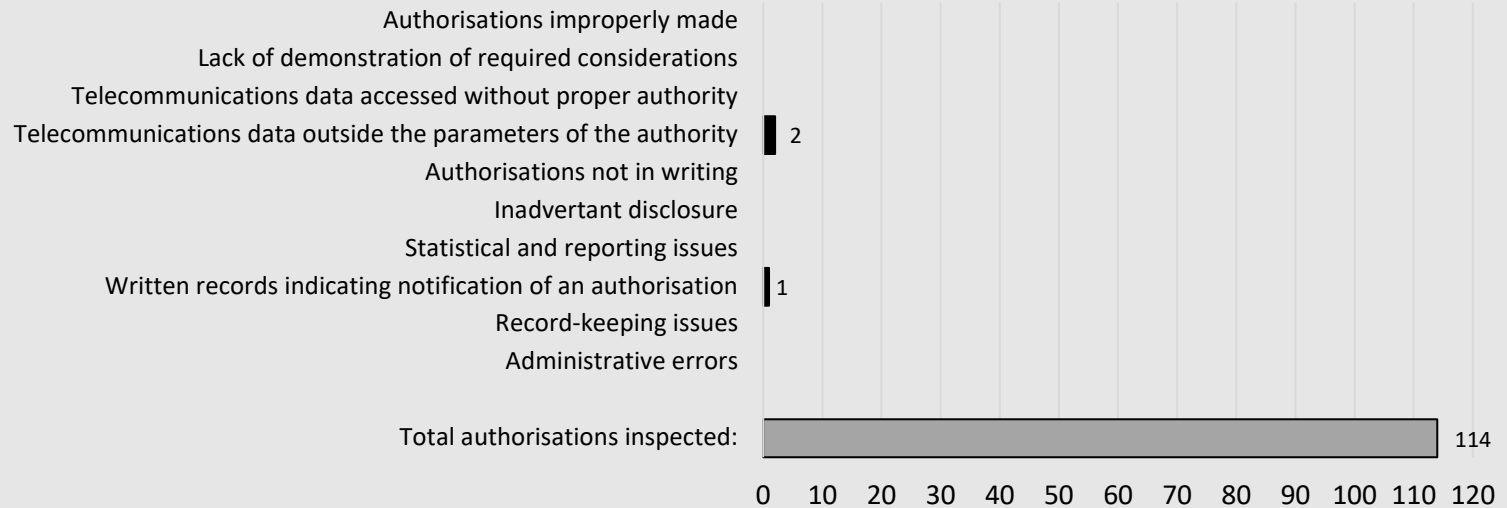
Disclosed
Identified



*The NSW Police disclosed one instance regarding record-keeping issues where it was unable to account for any potential use and communication of accessed stored communications as it could not locate the disc on which the stored communications was stored.

Telecommunications data findings

Northern Territory Police Instances identified during 2017–18

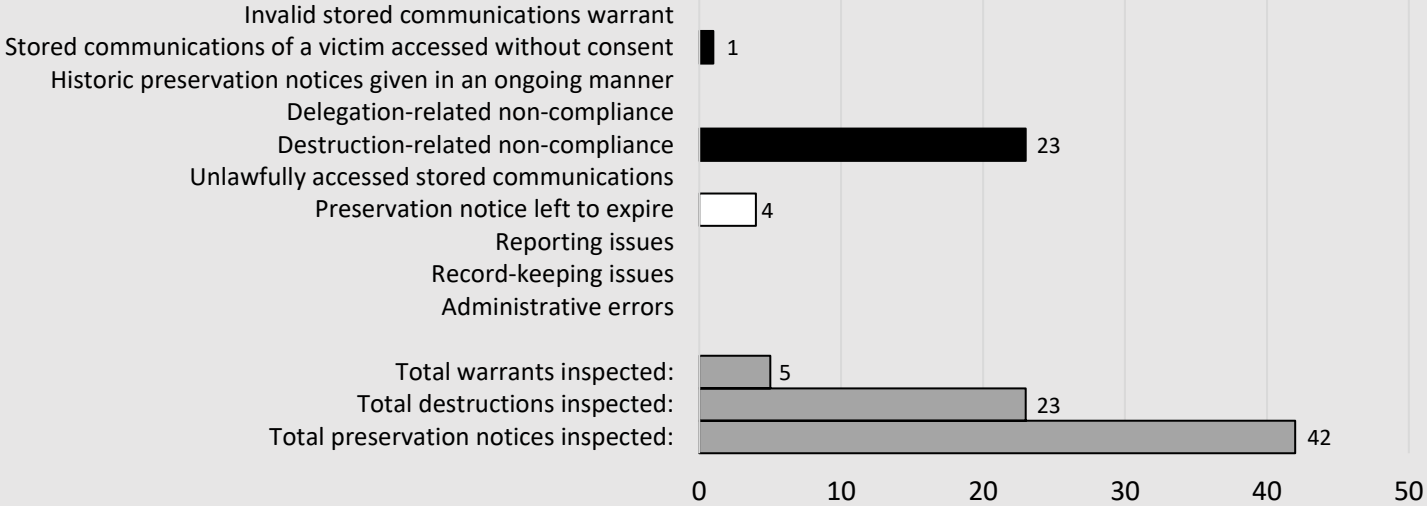


Stored communications findings

Northern Territory Police

Instances disclosed or identified during 2017–18

Disclosed
Identified

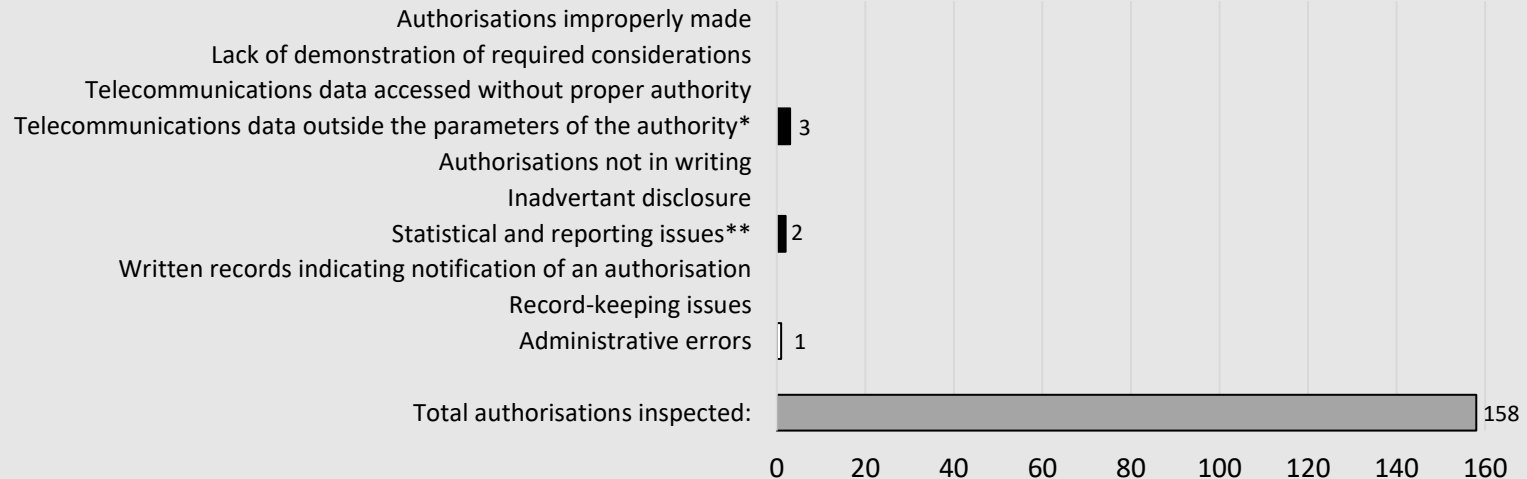


Telecommunications data findings

Queensland Police Service

Instances disclosed or identified during 2017–18

Disclosed
Identified



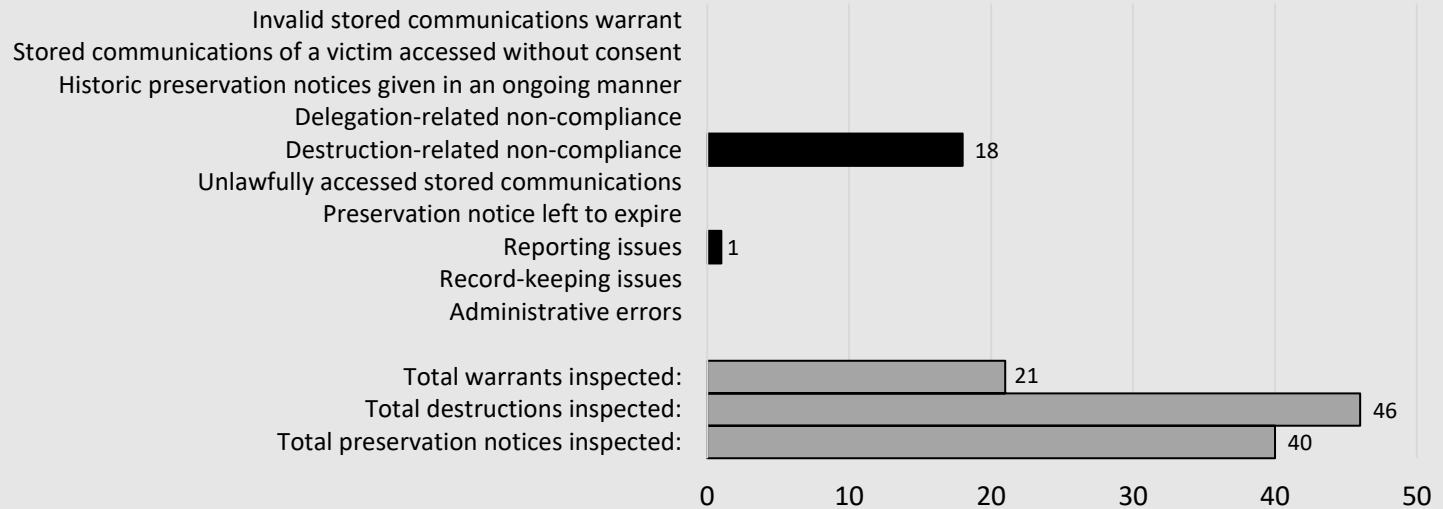
*In one instance regarding telecommunications data outside the parameters of the authority, our Office was unable to determine whether the telecommunications data received from the carrier was within the parameters of the authority because the carrier had not specified the telecommunications service to which the information related.

**Regarding statistical and reporting issues - due to a carrier-related issued which required QLD Police to re-notify a number of authorisations, the authorisations were erroneously reported to the Minister on two occasions. In a separate issue, due to the way in which QLD Police had compiled its report to the Minister, the number of historic authorisations reported was incorrect. We suggest to the QLD Police that it should consider methods to accurately report the number of authorisations made, as required by s 186.

Stored communications findings

Queensland Police Service

Instances identified during 2017–18



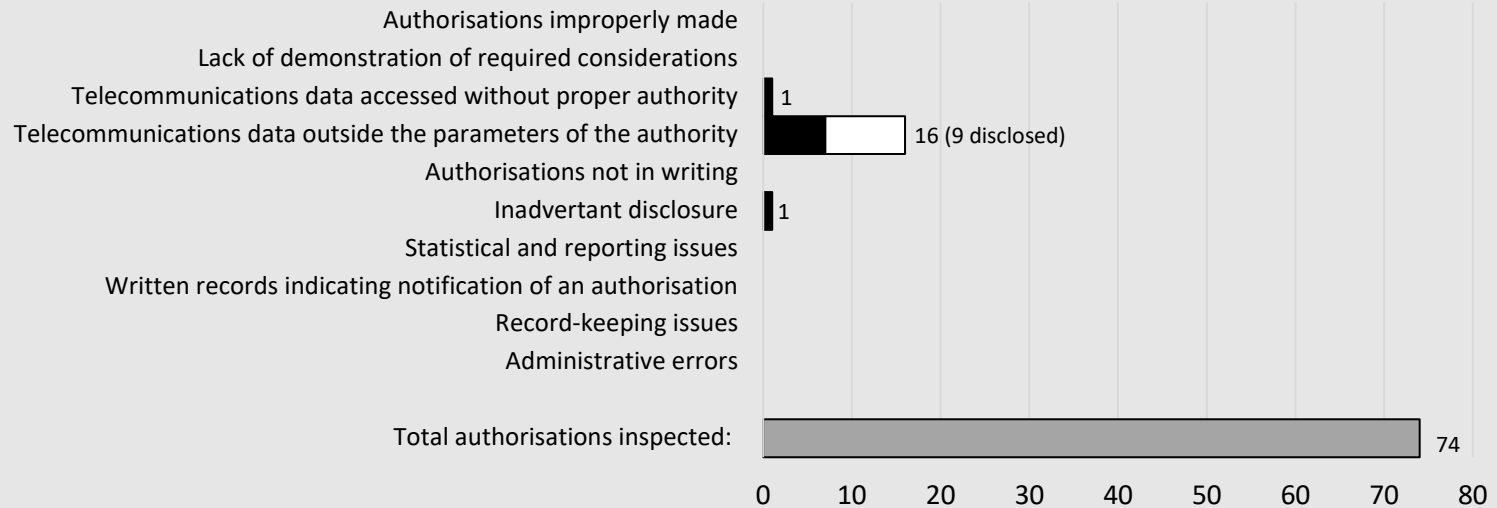
Telecommunications data findings

Disclosed
Identified



Independent Commission Against Corruption (South Australia)

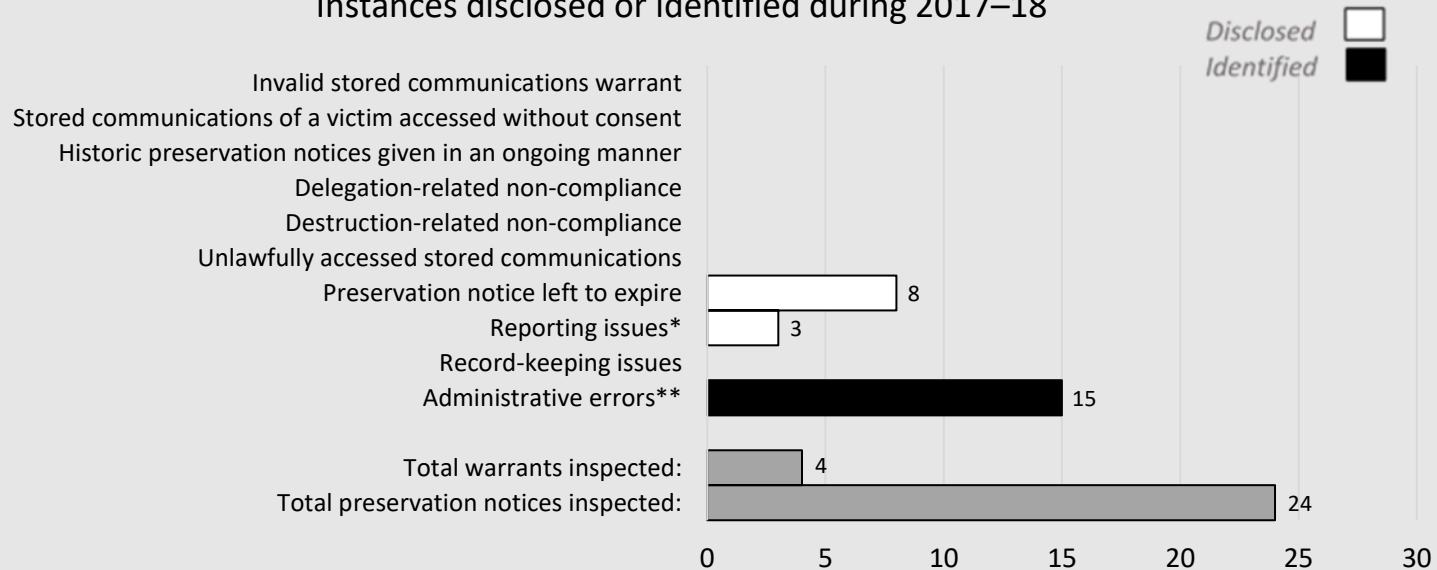
Instances disclosed or identified during 2017–18



Stored communications findings

Independent Commission Against Corruption (South Australia)

Instances disclosed or identified during 2017–18



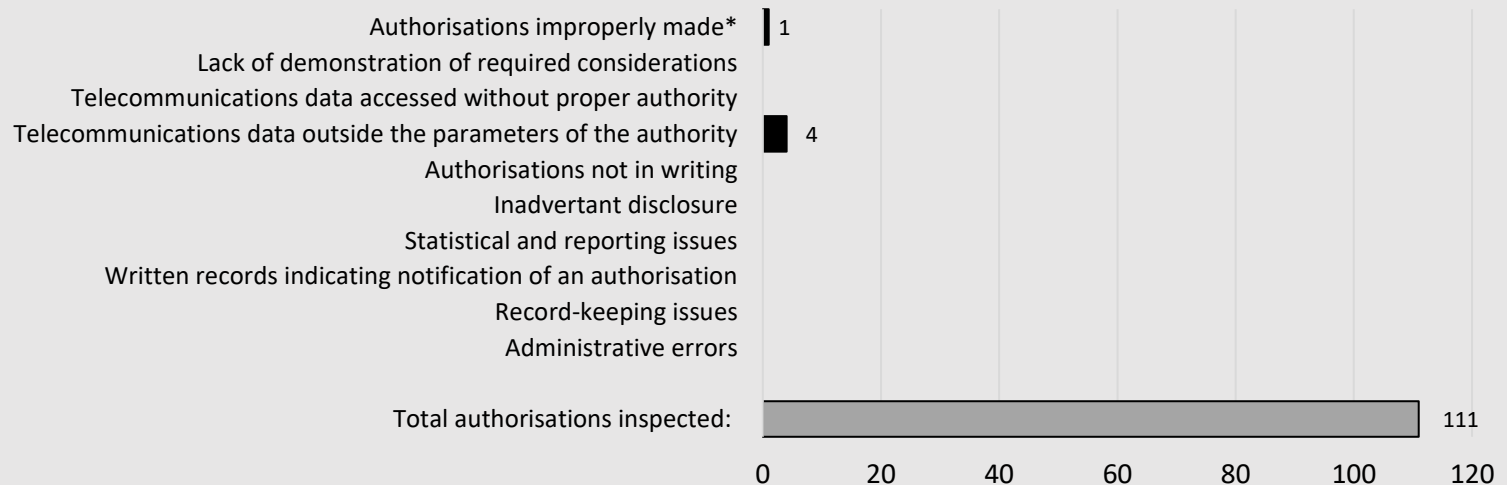
*Regarding reporting issues - during 2016–17 ICAC (SA) erroneously advised it had not given any preservation notices in the relevant period. When ICAC (SA) identified this error it advised our Office of the preservation notices it had given and these were inspected during our 2017–18 inspection.

**Regarding administrative errors - minor typographical error on each inspected ongoing domestic preservation notice. ICAC (SA) has since amended its template.

Telecommunications data findings

South Australia Police

Instances identified during 2017–18





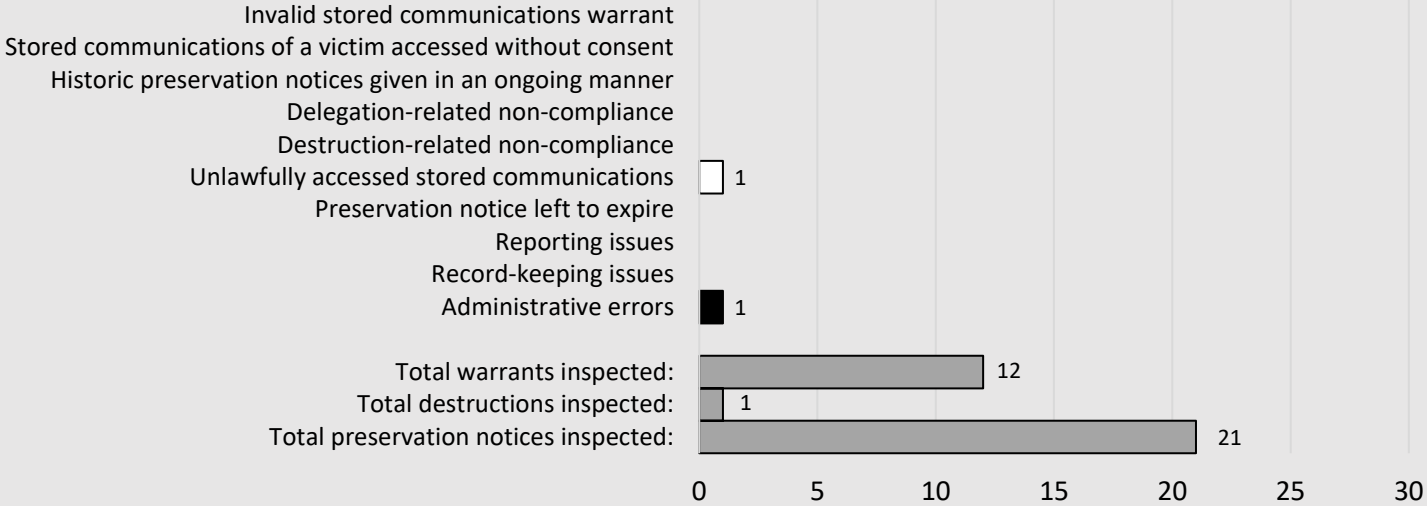
*In regards to the instance of authorisation improperly made, a prospective authorisation stated an expiry of 47 days after the authorisation was made. We note that in this instance SA Police calculated the period of the authorisation from when the authorisation was notified, which was one day after it was made. SA Police advised it would obtain legal advice in relation to this issue.

Stored communications findings

South Australia Police

Instances disclosed or identified during 2017–18

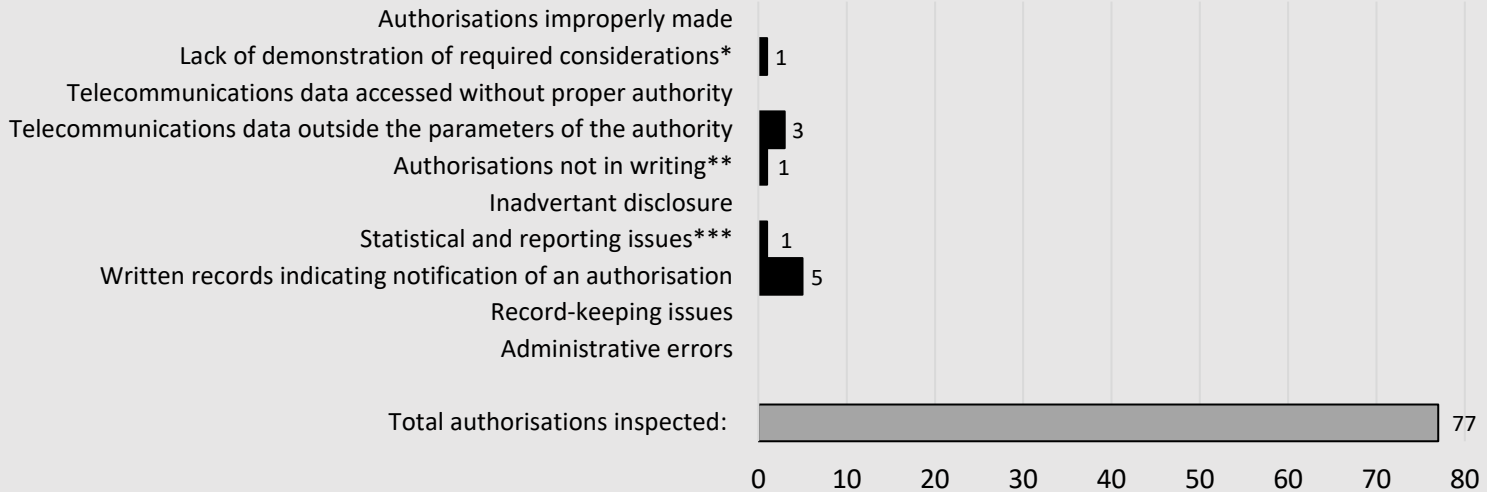
Disclosed 
Identified 



Telecommunication data findings

Tasmania Police

Instances identified during 2017–18



*Lack of demonstration of the required considerations discussed at page 16 of this report.

**Authorisations not in writing discussed at page 25 of this report.

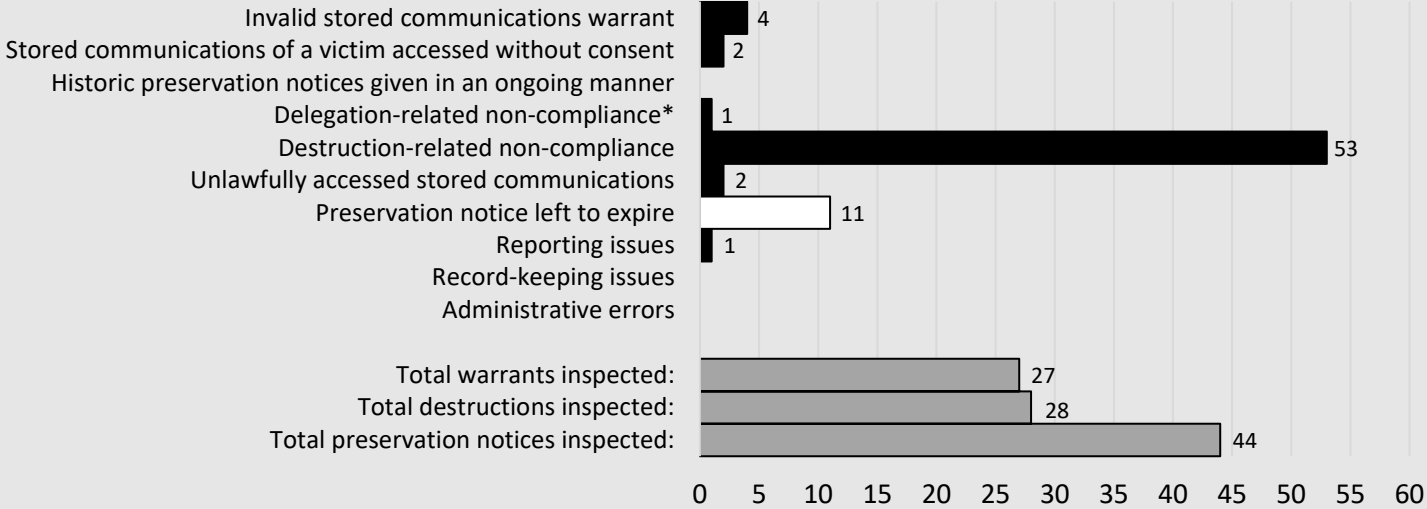
***Regarding statistical and reporting issues - during the inspection we identified that, due to a gap in processes, the number of authorisations reported to the Minister under s 186 did not account for all authorisations made within a specific area of TAS Police. TAS Police advised that it would amend its processes to ensure all authorisations made are correctly reported to the Minister.

Stored communications findings

Tasmania Police

Instances disclosed or identified during 2017-18

Disclosed
Identified

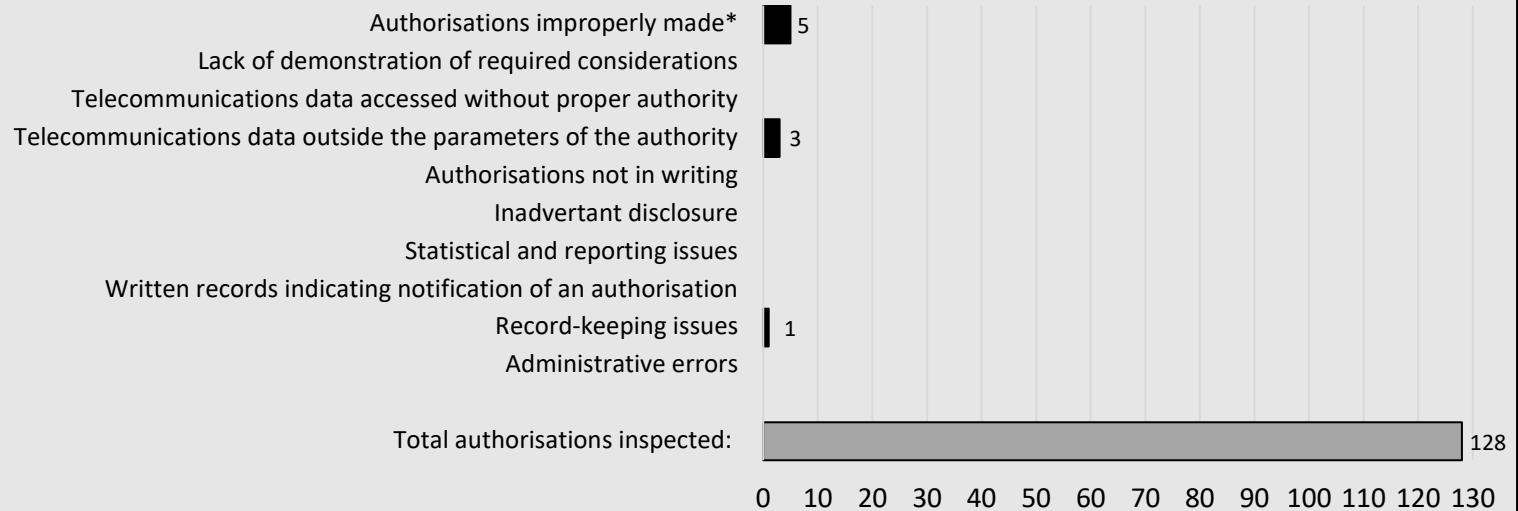


*Delegation-related non-compliance discussed at page 35 of this report.

Telecommunications data findings

Victoria Police

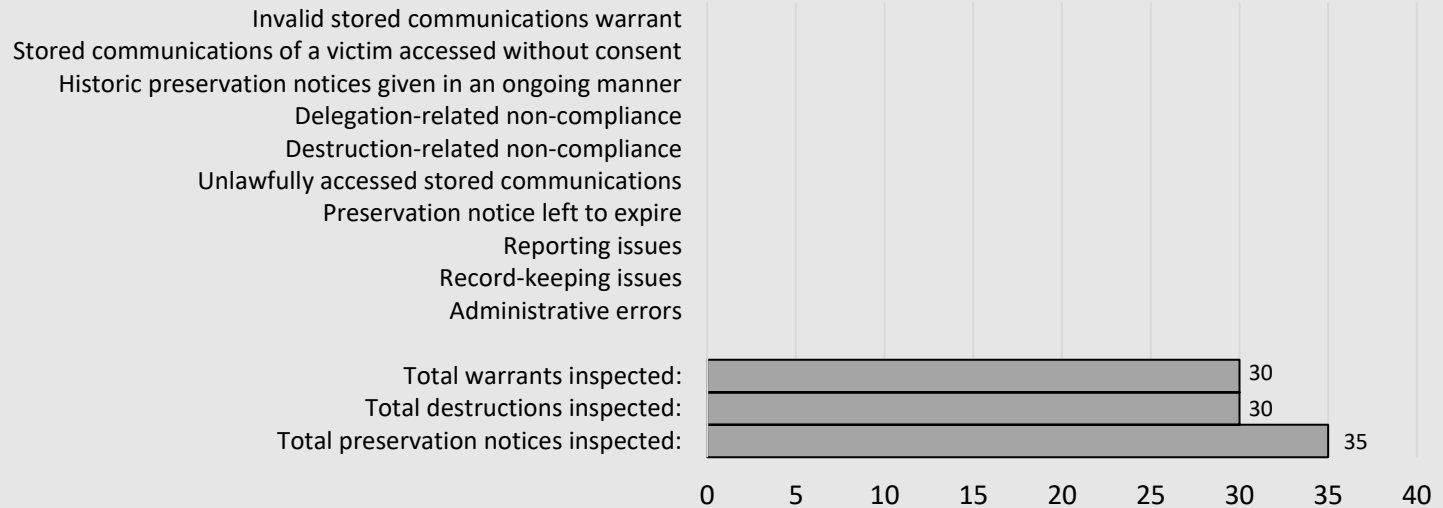
Instances identified during 2017–18



*Authorisations improperly made discussed at page 15 of this report.

Stored communications findings Victoria Police

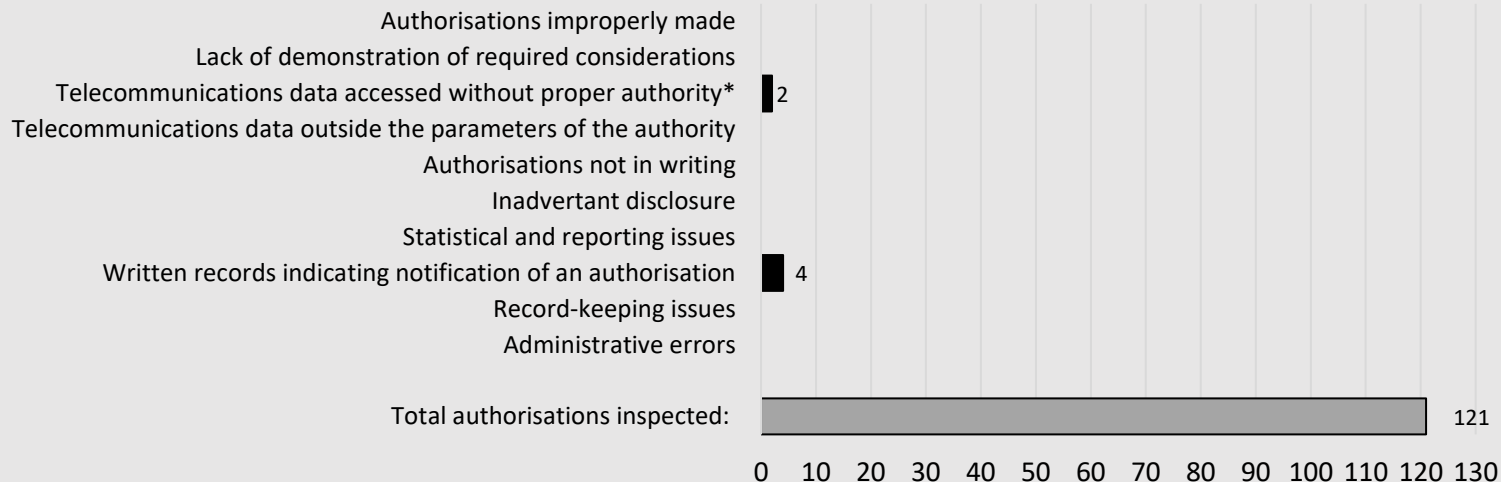
Nil instances of non-compliance identified or disclosed during 2017–18



Telecommunications data findings

Western Australia Police

Instances identified during 2017–18

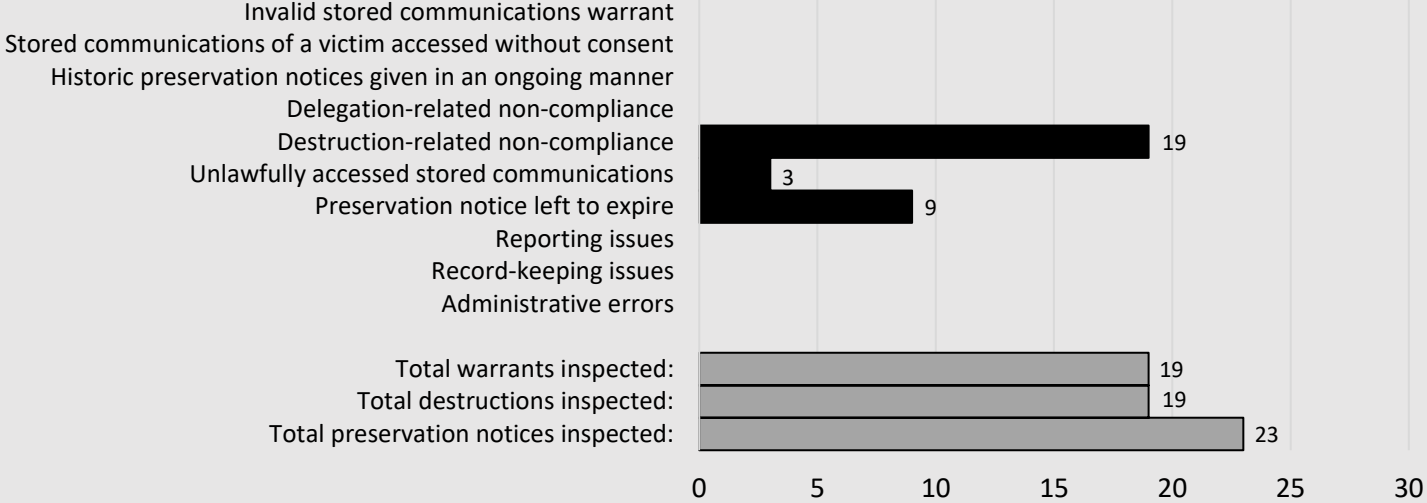


*In two instances of telecommunications data accessed without proper authority, we identified authorisations that included two distinct dates indicating when the authorisation was made. On both of these authorisations there was one date typed on the authorisation, being the same day the authorisation was notified, and another date, written by hand, being the day after the authorisation was notified. For this reason, in both instances, we were unable to determine the actual date the authorisation was made and, consequently, whether an authorisation was in place at the time the carrier was notified of the authorisation.

Stored communications findings

Western Australia Police

Instances identified during 2017–18



Appendix A – Telecommunications data inspection criteria: 2017–18

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

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

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

Process checks:

- Does the agency have effective procedures in place to ensure that authorisations are properly applied for, and are they sufficient?
- Does the agency have effective controls, guidance and/or training in place for authorised officers to ensure that authorisations are properly given?
- Does the agency have effective procedures in place to revoke prospective authorisations when required and notify carriers of any revocations?

Record checks in the following areas:

- Whether authorisations complied with the form and content requirements as determined by the Communications Access Coordinator (s 183(1)(f)).
- Whether authorisations were made by officers authorised under s 5AB.
- Whether authorisations were made in relation to specified information or documents (ss 178 to 180).
- Whether authorised officers have considered privacy in accordance with s 180F.

Specific to prospective authorisations

- Whether prospective authorisations are in force only for a period permitted by s 180(6).
- Whether prospective authorisations were revoked in relevant circumstances (s 180(7)).

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

Process checks:

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

Record checks in the following areas:

- Whether telecommunications data obtained by the agency was within the parameters of the authorisation.
- Whether the agency identified any telecommunications data (including content) that did not appear to have been lawfully disclosed and, if appropriate, sought clarification from the carrier and quarantined the data from use.

1.3 Were foreign authorisations properly applied for, given, extended and revoked? [AFP only]

Process checks:

- Does the agency have effective procedures in place to ensure that foreign authorisations are properly applied for, given, extended and revoked, and are they sufficient?

Record checks in the following areas:

- Whether authorisations for telecommunications data on behalf of a foreign law enforcement agency were properly given and disclosed (ss 180A to 180E).
- Whether foreign prospective authorisations were properly revoked in accordance with s 180B(4).
- Whether extensions of foreign prospective authorisations were properly made in accordance with ss 180B(6) and (7).

2. Has the agency properly managed telecommunications data?

Process checks:

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

Record checks in the following areas:

- **Spot Check:** Whether the use and disclosure of telecommunications data can be accounted for in accordance with s 186A(1)(g).

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

3.1 Did the agency properly apply for journalist information warrants?

Process checks:

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

Record checks in the following areas:

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

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

Record checks in the following areas:

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

3.3 Did the agency revoke journalist information warrants when required?

Process checks:

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

Record checks in the following areas:

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

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

Process checks:

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

Record checks in the following areas:

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

5. Was the agency cooperative and frank?

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

Appendix B – Stored communications inspection criteria: 2017–18

Inspection objective: To determine the extent of compliance with Chapter 3 of the *Telecommunications (Interception and Access) Act 1979* by the agency and its officers.

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

1.1 Were stored communications properly applied for?

Process checks:

- Does the agency have effective procedures in place to ensure that warrants are properly applied for and issued in the prescribed form (s 118(1))?

Record checks in the following areas:

- Whether applications for stored communications warrants were made in accordance with ss 110 to 113, or ss 111, 114 and 120(2) for telephone applications.
- Whether the warrant was only in relation to one person (s 117).
- If the application relates to the same telecommunications service as a previous warrant—whether the application was made in accordance with s 119(5).
- Whether a connection can be established between the person listed on the warrant and the relevant telecommunications service (s 117).

1.2 Was the authority of the warrant properly exercised?

Process checks:

- Does the agency have effective procedures and authorisations in place to ensure the authority of the warrant is properly exercised?

Record checks in the following areas:

- Whether the authority of the warrant was exercised in accordance with s 127.

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

Process checks:

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

Record checks in the following areas:

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

2. Has the agency properly managed accessed stored communications?

2.1 Were stored communications properly received by the agency?

Process checks:

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

Record checks in the following areas:

- Whether stored communications were received in accordance with s 135.

2.2 Were stored communications properly dealt with and destroyed?

Process checks:

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

Record checks in the following areas:

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

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

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

Process checks:

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

Record checks in the following areas:

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

3.2 Did the agency revoke preservation notices when required?

Process checks:

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

Record checks in the following areas:

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

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

Process checks:

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

Record checks in the following areas:

- Whether the agency has kept records in accordance with s 151.

5. Was the agency cooperative and frank?

- Is there a culture of compliance?
- Was the agency proactive in identifying compliance issues?
- Did the agency disclose issues?
- Were issues identified at previous inspections addressed?