COMMONWEALTH OMBUDSMAN

Surveillance devices and computer access: What's happening with your information?

Report to the Attorney-General on agencies' compliance with the *Surveillance Devices Act 2004* (Cth) for Ombudsman inspections conducted from 1 July to 31 December 2023

Report by the Commonwealth Ombudsman, Iain Anderson under section 61 of the *Surveillance Devices Act 2004* (Cth)

March 2024

Contents

Our Report – At a glance

A **surveillance device warrant** permits law enforcement to use surveillance devices in criminal investigations or to locate and safely recover a child to whom recovery orders relate.

There are four types of surveillance devices: **tracking devices, optical surveillance devices, listening devices** and **data surveillance devices**. Some devices are a combination of two or more devices.

A **computer access warrant** permits law enforcement to collect information from a computer to obtain evidence for a criminal investigation or to locate and safely recover a child to whom recovery orders relate.

A **data disruption warrant** allows access to data held in a target computer to identify, disrupt, and copy the data, if doing so is likely to assist in frustrating the commission of a relevant offence.

IMPROVEMENTS WE NOTICED

Most agencies demonstrated a strong compliance culture and engaged positively with us. We received proactive disclosures of non-compliance and observed regular updates and reviews of procedures and guidance materials.

NON-COMPLIANCE RISKS WE OBSERVED

We observed inadequacies with the review and destruction of protected information holdings, insufficient recording of decisions and failures within some agencies to revoke warrants or deactivate surveillance devices.

EMERGING ISSUES WE WILL MONITOR

We will continue to monitor the insufficient recording of decisions to use surveillance device powers and difficulties within agencies to maintain compliance resourcing and expertise.

Executive summary

The *Surveillance Devices Act 2004* (the Act) enables law enforcement to lawfully apply for and use powers to covertly gather evidence of a relevant offence, or for another specified purpose under the Act, by using a surveillance device or accessing a computer. The Act specifies how agencies will deal with the information obtained and applies restrictions on any unlawful recording, use or communication of this information.

The use of a device to covertly listen, track or observe a person or access their computer is highly intrusive of a person's privacy and freedom of movement. Often the person subject to this surveillance is unaware that such a device has been used against them and cannot complain or question an agency's actions.

The Office of the Commonwealth Ombudsman's (the Office) oversight of law enforcement agencies' use of these powers is an important community safeguard. Between 1 July and 31 December 2023, we inspected how the following agencies used the powers under the Act:

- Australian Criminal Intelligence Commission (ACIC)
- Australian Federal Police (AFP)
- Law Enforcement Conduct Commission (LECC), and
- National Anti-Corruption Commission (NACC).

This included reviewing the records of these agencies from 1 July 2022 to 30 June 2023.

This report provides a summary of the most significant findings from these inspections and also identifies matters that will assist agencies to improve their compliance with the legislation, such as the adequacy of their policies and procedures. While our inspections reviewed agencies' use of computer access and data disruption warrants, our most significant findings relate to their use of surveillance device warrants.

Responsible management of surveillance devices powers

The responsible use and administration of these powers stems from good governance, accountable decision making, continuous review of protected information and a strong compliance culture.

We found examples of good practice across each of the agencies we inspected, with all agencies having either a maturing or mature compliance culture[1].

The NACC was a stand-out in terms of improvements, having completed a wholesale review of its policies, processes, training and systems during its establishment phase. While this placed the agency in a strong position to use the powers, anticipated growth to its investigative workforce will be a key risk the NACC will need to manage in maintaining this mature compliance culture.

Room to Improve

We observed non-compliance and risks in agency practices and records that needed immediate attention.

Inadequate review of protected information

We are concerned that the ACIC is continuing to hold protected information, which is likely to be older than 5 years and unlikely to relate to any civil or criminal proceeding, in a legacy exhibit system. The ACIC also disclosed a second legacy system which may hold protected information requiring review. We recommended that the ACIC immediately review this material and destroy any protected information that should not be retained under the provisions of the Act.

Limitations in destroying protected information

The LECC and NACC use a similar case management system. While both agencies regularly authorise the destruction of protected information, their

[1] AFP and NACC were assessed as having a 'Mature' compliance culture. The LECC was assessed as being 'Maturing' to 'Mature', while ACIC was considered 'Maturing'.

system was unable to purge these records. We were satisfied steps had been taken to rectify this deficiency and, in the meantime, records authorised for destruction had been quarantined, but suggested the agencies prepare these records for a bulk purge from the system once the software update has been implemented.

Failure to revoke warrants or deactivate surveillance devices

We found instances at the AFP and LECC where warrants were not revoked after the device was deactivated. We also discovered one instance where the ACIC failed to deactivate a device after the warrant was revoked. While we acknowledge operational circumstances may exist where the warrant may be required to be retained, from the records we inspected we found the retention of the warrant, in most instances, was not justified. The ACIC self-disclosed the incident to our Office. We reviewed the incident and were satisfied that no unauthorised protected information had been collected through the device.

We made several suggestions for agencies to revise their policies and practices to ensure warrants are revoked when they were no longer required or where a surveillance device had been deactivated.

Emerging Issues – Recording critical decisions and retaining expertise

We identified two emerging issues that we will continue to monitor. These include:

- consistency in recording the decision to apply for a surveillance device or computer access warrant, particularly in demonstrating considerations of necessity, proportionality and reasonableness before using the powers, and
- sufficiency of resourcing and staff turnover in Compliance Teams presenting risks to agencies ability to meet their obligations and mature their compliance culture.

Scope and methodology

Section 55(1) of the *Surveillance Device Act 2004* (the Act) requires the Ombudsman to inspect the records of a law enforcement agency to determine the extent of their compliance with the Act.

Section 61(1) of the Act requires the Ombudsman to provide reports to the Minister (the Attorney-General) at 6 monthly intervals with the results of each inspection conducted during the reporting period. These reports provide transparency to the Attorney-General and the public about how agencies use these intrusive powers.

How we oversee agencies

We take a risk-based approach to our inspections. We focus on areas where agencies are, or may be, at risk of not complying with legislative requirements or best practice standards, and where non-compliance would cause public harm. Our inspections may include reviewing a selection of the agency's records, having discussions with relevant agency staff, reviewing policies and processes, and assessing any remedial action the agency has taken in response to issues we have previously identified with them.

This report presents our findings on the most significant risks we reviewed, particularly risks that:

- a surveillance device is not deployed and used in a manner consistent with the warrant
- surveillance device records (including protected information) and reports are not appropriately reviewed and destroyed
- timelines for destroying protected information are not adhered to
- appropriate considerations were not given to the necessity and proportionality of using a surveillance device or access to a computer prior to the warrants being sought, and
- governance and policy documents across agencies are not fit for purpose.

We do not comment in this report on administrative issues or instances of non-compliance where the consequences are low risk and of minimal impact to the community.

Our inspections may identify a range of issues from minor administrative errors through to serious non-compliance that affects an individual's rights (notably privacy), the validity of evidence collected, or systemic issues. If an issue is sufficiently serious or systemic, or was previously identified and not resolved, we may make formal recommendations for remedial action. Where an issue of non-compliance is less serious or was not previously identified, we generally make suggestions to the agency to address the non-compliance and to encourage them to identify and implement practical solutions. We may also make suggestions or comments where we consider an agency's existing practice may expose it to compliance risks in the future.

To ensure procedural fairness, we give agencies the opportunity to respond to our inspection findings before consolidating the significant findings into this 6-monthly report to the Attorney-General.

We follow up on any remedial action agencies have taken to address our recommendations and suggestions at our next inspection.

Findings

Good compliance culture = Responsible use of powers

Strong Compliance Culture

The NACC commenced during this inspection period. We were pleased to see the NACC used the period during which the Australian Commission for Law Enforcement Integrity (ACLEI) transitioned into the NACC to conduct a wholesale review of their processes and governance. This included building on the previous experiences of ACLEI and making the improvements required to support the NACC's inception.

A mature compliance culture stems from a **proactive approach to ensuring processes, governance and training programs are contemporary and fit for purpose**. This was evident at the NACC.

We found the NACC to have regular structured training, including e-Learning modules available to all staff, demonstrating a strong commitment to fostering a culture of compliance. Further, the NACC incorporated quality assurance processes into their new case management system and built the systems to be 'future ready' for the NACC's operations. We commend the NACC on having a positive and proactive attitude to compliance and encourage agencies to model this approach.

Similarly, we observed the AFP to have a strong compliance culture through its internal decision-making on the necessity for surveillance devices and digital surveillance prior to applying for warrants. While applied less formally, LECC and ACIC also applied similar decision-making practices. These processes include checking applications, affidavits and warrants by supervisors, independent

superintendents, and compliance teams to ensure sufficient consideration was given to privacy, necessity, proportionality and reasonableness before use of the powers.

Positive engagement, proactive disclosure

Across all agencies, we experienced positive engagement with our office in the lead up to and during inspections. We found agency staff to be open, helpful in answering our questions and assisting with access to what we needed. For example, where the AFP found instances of non-compliance, they were open and forthcoming with these disclosures and demonstrated their controls to identify, assess and respond to affected records.

We continue to see proactive disclosure of non-compliance across all agencies, indicating a willingness to engage openly with our office and remain transparent and accountable in their use of the powers. We appreciate the frankness and openness of agency staff during inspections and value the shared commitment to robust oversight of surveillance device powers.

Procedures and guidance materials

We found each agency had amended their standard operating procedures and guidance material in response to our concerns with destruction processes, and to ensure agency staff are aware of their obligations under section 46 of the Act.

Under section 46(1)(b)(i) of the Act, the chief officer must cause the destruction of any record or report comprising protected information as soon as practicable if satisfied that no civil or criminal proceeding to which the material relates has been, or is likely to be, commenced. The exception to this is where that material is still required in connection with an activity or purpose prescribed under the Act.

The Act does not define 'as soon as practicable' and agencies should have internal guidance on what is an appropriate timeframe to satisfy the destruction requirements. If there is no internal guidance, we consider a period of up to 28 days is generally appropriate.

At the LECC, we found that they should clarify the interpretation of 'as soon as practicable' in their standard operating procedures, to minimise the risk that they would not comply with revocation and destruction timeframes under the Act. The LECC accepted this finding and committed to updating their guidance material. Additionally, we noted significant work had been undertaken by the LECC since our last inspection to improve their standard operating procedures and investigation management processes, particularly in mitigating risks of inappropriate or disproportionate use of surveillance device powers. While some policies were still in draft and training was required, the LECC's governance framework was developing to support the use of the powers.

We found the AFP had introduced a range of governance, templates, procedures, and training to support officers using surveillance device powers. While this significantly mitigates risks of failing to destroy protected information that is no longer required, we also considered it to be a significant factor in building a more mature compliance culture across the AFP's workforce.

Despite our concerns with the ACIC's handling of legacy exhibits containing protected information, discussed later in this report, we found the ACIC to have sound guidelines for the destruction of current material and timely consideration of whether to destroy material regularly occurs. We also noted the ACIC showed a proactive approach to improving compliance with other requirements of the Act during the inspection period.

Room to improve

We found insufficient efforts to review and destroy protected information, limitations in case management systems to purge records, and failures to revoke warrants as areas that required the most improvement.

We also observed several issues where further efforts by agencies could reduce the level of risk of non-compliance and public harm to the community. Two issues emerged including the recording of critical decisions and fostering continuity in compliance resourcing and expertise.

Handling Protected Information

Protected Information is defined under section 44 of the Act. In broad terms, it is includes:

- any information obtained from the use of a surveillance device or access to a computer under a warrant or authorisation
- any information relating to the application, issue or execution of a warrant or authorisation, and
- any information likely to enable identification of a person, object or premise subject to a warrant or authorisation.

The regular review of protected information for either retention or destruction is critical to the responsible use of the powers. Section 46 of the Act requires agencies to destroy protected information as soon as practicable, and within 5 years of its creation, once the chief officer is satisfied that the material is not required for a civil or criminal proceeding for which it was relates to. Protected information may be kept longer than 5 years, but the chief officer must be satisfied that the material relates to ongoing or likely civil or criminal proceedings.

Inadequate review and destruction of protected information

Protected information gathered through a surveillance device is highly intrusive of a person's privacy. While the Act enables law enforcement to gather and use

such material to support civil or criminal proceedings, it is incumbent on these agencies to destroy this information when it is no longer required for a purpose under the Act. Section 46 is a key safeguard in the legislation, and we consider it responsible practice by agencies to review the need to retain such information at the completion of any related civil or criminal proceedings. If the material is retained post these proceedings for a purpose under the Act, then the agency should review the material within 5 years of obtaining the protected information.

At the ACIC, we found significant amounts of protected information contained in a legacy exhibit system that had not been reviewed for retention or destruction in accordance with section 46. The protected information in these exhibits was unlikely to relate to any civil or criminal proceeding, creating a serious risk of the ACIC retaining the material for purposes not permitted under the Act. The ACIC's advice that it would take up to 7 years to review these legacy holdings (to determine whether the protected information should be retained or destroyed), was unacceptable.

The ACIC also disclosed another legacy tracking device system that may hold protected information. We understand that there are up to 105 warrants and tracking device authorisations that need to be assessed to determine if there is any protected information on this system. If so, these records are likely to have been retained for 5 years or more and should be a priority for review. The ACIC's inability to be certain as to whether the server contained protected information is an issue we will continue to pursue with the ACIC.

We **recommended** that the ACIC prioritise and resource the review and, where necessary, immediately destroy protected information contained.

The ACIC acknowledged our recommendations and confirmed protected information is also contained on a legacy tracking device system. The ACIC advised they will review legacy holdings over the next 18 months and will implement measures to review the protected information contained within the

legacy tracking device system, to determine whether the material should be retained or destroyed. The ACIC is developing a new National Exhibit Management system with built-in compliance controls to ensure protected information is reviewed at regular intervals.

Limitations of systems to destroy protected information

The LECC and the NACC use a similar case management system. We identified the limitations in the system which prevented either agency being able to purge protected information and records from their consolidated holdings. This makes it difficult for the agencies to destroy protected information compliantly with the Act.

We are comfortable that the agencies have taken reasonable steps to review, and quarantine protected information authorised by the chief officer for destruction. The agencies and the vendor of the system both assured our Office that a solution to remove protected information from the system would be introduced in early 2024. Until this capability is delivered, there is an ongoing risk of protected information being retained post the expiry of a relevant purpose. While we will continue to monitor agencies efforts to progress these system updates, we also suggested that they prepare quarantined records already authorised to be destroyed for purging from the system once the updates are in place.

Failure to revoke warrants or discontinue the use of surveillance devices

We found the AFP and LECC failed to revoke surveillance device warrants in accordance with sections 20 and 21 of the Act. We also found one instance where the ACIC failed to discontinue a device after the warrant was revoked.

If the use of a surveillance device under a warrant is no longer required for the purpose it was sought, sections 20 and 21 require the Chief Officer of the agency to revoke the warrant and take steps to discontinue the use of the surveillance device. We expect agencies to do this as soon as practicable and within 28 days of being satisfied that the surveillance device is no longer required.

Law enforcement officers must also immediately inform the chief officer if they believe the use of a surveillance device under a warrant is no longer necessary for its original purpose. Similar requirements apply in relation to computer access warrants under sections 27G and 27H.

At the LECC, we found instances where multiple surveillance device warrants were not revoked when it became clear that the surveillance device under the warrant was no longer required. While the surveillance devices were deactivated so they could not be used, the warrants were allowed to continue until they naturally expired. We suggested that the LECC revoke any surveillance device warrants or computer access warrants within 28 days of the surveillance device or access to a computer being discontinued. Additionally, although the LECC's draft standard operating procedure (SOP) reflects that both the warrant should be revoked and use of the surveillance device should be discontinued, we suggested the SOP be updated to specify that this should occur within 28 days of being satisfied the surveillance device is no longer required. The LECC accepted this suggestion and committed to update their policies to include the definition of 'as soon as practicable' to mean within 28 days.

The AFP self-disclosed multiple instances where surveillance device warrants had not been revoked in accordance with section 20 of the Act and their own internal policies. We noted the AFP set an admirable internal threshold of 5 days to revoke the warrant once the chief officer is satisfied the surveillance device is no longer required for the purpose for which it was sought. Despite this, five warrants disclosed to our Office had exceeded 28 days before being revoked. We suggested the AFP take the steps necessary to ensure warrants are revoked in accordance with sections 20 and 21(2) of the Act. The AFP accepted this suggestion.

Our findings at the ACIC were slightly different. We found the ACIC failed to discontinue a surveillance device after the warrant was revoked, thereby creating a risk of obtaining unauthorised protected information. We reviewed the circumstances around this warrant and were satisfied that no unauthorised

protected information had been collected through the active device. In this instance, we acknowledged that it appeared to be a one-off instance and were satisfied it was not indicative of systemic issues. No remedial action was required.

Emerging Issue – Insufficient recording of critical decisions

We noted the LECC's practice of convening a pre-warrant meeting with relevant directors, managers, case lawyers, specialist capabilities and the case officer to review investigative strategies and requirements for a surveillance device or computer access warrant. Like the AFP's pre-warrant vetting practices, we consider this good practice and reflects responsible consideration of necessity and proportionality prior to seeking a surveillance device warrant. We noted however, that records are not kept from this meeting nor are any critical decisions to pursue a surveillance device or computer access warrant recorded. We also understand that the LECC do not use critical decision logs for most investigations.

The decision to approve seeking a surveillance device has significant impacts on the resourcing, direction and level of privacy intrusion of an investigation. This is a critical decision that should be recorded, to reflect the considerations made when considering applications for surveillance devices or computer access warrants. The LECC agreed with this view and will implement critical decision records within their case management system.

Emerging Issue – Maintaining compliance resourcing and expertise

We noted that a turnover of compliance staff at the LECC impacted consistency in compliance activities and reporting. The LECC also recognised the risks to compliance and had taken steps to address this capability gap, including enhancing the engagement between compliance and investigative teams to foster greater continuity and consistency in compliance and reporting. The LECC had also taken steps to retain or recruit expertise in their compliance team which would reduce the likelihood of future non-compliance through deficient administration of the powers. We support the view taken by the LECC that strong internal communication leads to increased compliance through the sharing of knowledge, expertise and general awareness.

We observed that resource limitations and competing priorities were limiting the ACIC's destruction of protected information.

We **recommended** that ACIC ensure sufficient resources and priority were allocated to ensure the agency meets its obligations with destroying protected information. As reported above, the ACIC acknowledged this recommendation.

While we acknowledge the NACC is in a strong position to use the powers under the Act going forward, we noted that the anticipated growth to its investigative workforce over the next 12-18 months will be the NACC's greatest risk to consistency in compliance and maintaining a mature compliance culture. The NACC recognised this potential risk and anticipated increasing its induction and training of new members entering the agency to mitigate this risk.

Appendix A

Table 1 – inspection findings

Agency and inspection date	Findings, Recommendations, Suggestions, Comments
LECC 16-18 October 2023	Findings: 4 Recommendations: 0 Suggestions: 4 Comments: 3
AFP 3-5 October 2023	Findings: 3 Recommendations: 0 Suggestions: 3 Comments: 2
ACIC 5-6 October 2023	Findings: 2 Recommendations: 2 Suggestions: 0 Comments: 0
NACC 19-20 October 2023	Findings: 0 Recommendations: 0 Suggestions: 0 Comments: 0

Table 2 – summary of records inspected

	Records made available	Records inspected
LECC	3 SD	3
	1 CAW	1
NACC	6	2
ACIC	30 SD	7
	4 TDA	4
	32 R	0
	194 D	10
	8 W – 5YO	8
AFP	626 SD	7
	11 SO	5
	23 RW	1
	15 TDA	2
	79 D	0
	129 DNE	0
	199 R	0
	7 CAW	4
	1 DDW	1

Key	SD	Surveillance device warrant
	CAW	Computer access warrant
	SO	Supervisory orders
	RW	Retrieval warrants
	TDA	Tracking device authorisations
	D	Destructions
	W – 5YO	Warrants with protected information obtained more than 5 years ago that has not been destroyed
	DNE	Destructions – not executed
	R	Retained
	DDW	Data disruption warrant