



Australian Government

Department of Home Affairs



Surveillance Devices Act 2004

Annual Report 2018–19

ISSN: 1833-4490 (Print)
ISSN: 2652-1660 (Online)

© Commonwealth of Australia 2019

With the exception of the Commonwealth Coat of Arms, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license at <https://creativecommons.org/licenses/by/4.0/legalcode>.

This means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website at <https://creativecommons.org/> as is the full legal code for the CC BY 4.0 license at <https://creativecommons.org/licenses/by/4.0/legalcode>

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed at the Department of Prime Minister and Cabinet website—
<https://www.pmc.gov.au/government/commonwealth-coat-arms>.

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

National Security Policy Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Surveillance Devices Act 2004

Annual Report 2018–19

Contents

| | |
|---|-----------|
| EXECUTIVE SUMMARY | 1 |
| Objects of the Act | 1 |
| Information relating to the administration of the Act | 2 |
| Legislative reforms | 2 |
| Key judicial decisions | 2 |
| Key findings | 3 |
| CHAPTER ONE – WARRANTS AND OVERSIGHT | 4 |
| Form of warrants | 5 |
| Thresholds to obtain warrants | 5 |
| Extraterritorial operation of warrants | 6 |
| Use of the information obtained | 6 |
| Accountability provisions | 7 |
| Inspections and reports by the Ombudsman | 7 |
| CHAPTER TWO – SURVEILLANCE DEVICES | 8 |
| Applications for surveillance device warrants | 8 |
| Remote applications for surveillance device warrants | 10 |
| Extension applications for surveillance device warrants | 10 |
| International assistance applications for surveillance device warrants | 12 |
| Applications for retrieval warrants | 13 |
| Remote applications for retrieval warrants | 13 |
| Use of surveillance devices without a warrant – emergency circumstances | 15 |
| Use of surveillance devices without a warrant – investigative purposes | 16 |
| Tracking device authorisations | 16 |
| CHAPTER THREE – COMPUTER ACCESS WARRANTS | 18 |
| Applications for computer access warrants | 18 |
| International assistance applications for computer access warrants | 20 |
| CHAPTER FOUR – EFFECTIVENESS OF THE ACT | 21 |
| CHAPTER FIVE – FURTHER INFORMATION | 23 |
| APPENDIX A – LIST OF TABLES | 24 |
| APPENDIX B – ABBREVIATIONS | 25 |

EXECUTIVE SUMMARY

The *Surveillance Devices Act 2004* (the Act) requires that each year the Minister for Home Affairs lay before each house of Parliament a report setting out the information required by section 50 of the Act. The Annual Report for 2018–19 describes the extent and circumstances in which eligible Commonwealth, State and Territory law enforcement agencies have used the powers available under the Act between 1 July 2018 and 30 June 2019.

Objects of the Act

The Act is intended to facilitate cross-border investigations and information sharing between Australian law enforcement agencies, and complements state and territory surveillance devices laws. It does not place constraints on the use of surveillance devices by the general public. Rather, it authorises the use of surveillance devices by law enforcement agencies. The Act provides a single legislative regime for Commonwealth agencies to use surveillance devices and a warrant framework to access data held in computers.

The Act also authorises state and territory law enforcement agencies to use surveillance devices and access data held in computers under the Commonwealth regime in defined circumstances.

The Act also operates to restrict the use, communication, and publication of information that is obtained through the use of powers under the Act by law enforcement agencies.

Powers under the Act may be used by officers of the following law enforcement agencies:

- Australian Federal Police (AFP)
- Australian Commission for Law Enforcement Integrity (ACLEI)
- Australian Criminal Intelligence Commission (ACIC)
- State and Territory police forces
- Crime and Corruption Commission of Queensland (CCC (QLD))
- Corruption and Crime Commission of Western Australia (CCC (WA))
- Independent Broad-based Anti-corruption Commission of Victoria (IBAC)
- Independent Commission Against Corruption of New South Wales (ICAC (NSW))
- Independent Commissioner Against Corruption of South Australia (ICAC (SA))
- New South Wales Crime Commission (NSW CC)
- New South Wales Law Enforcement Conduct Commission (LECC)

Information relating to the administration of the Act

Paragraph 50(1)(j) provides that the Minister may include information in the Annual Report on the administration of this Act, that he or she considers appropriate.

Legislative reforms

Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* amended the Act to introduce computer access warrants. Computer access warrants authorise law enforcement agencies to:

- covertly access devices to investigate serious crimes;
- search devices such as laptops, mobile phones and USBs, and collect information; and
- conceal the fact that a device has been accessed.

Law enforcement agencies may apply for computer access warrants when investigating ‘relevant offences’ which generally carry a maximum imprisonment term of at least three years. Further information regarding computer access warrants and statistics pursuant to their use during the 2018–19 reporting period are available in chapter three of this report.

Key judicial decisions

No significant judicial decisions relevant to the Act were handed down during the reporting period.

Key findings

The following key statistics are relevant to the 2018-19 reporting period:

- In 2018–19, law enforcement agencies were issued 740 surveillance device warrants, a decrease of 42 from the 782 issued in 2017–18. Six applications for surveillance device warrants were refused by nominated AAT members due to insufficient supporting evidence.
- The number of applications granted to extend surveillance device warrants has increased from 187 to 234. Applications to extend warrants are often due to the prolonged nature of investigations for complex and serious crime (where evidence gathering may not have been completed within the prescribed period of 90 days).
- 31 retrieval warrants were issued to law enforcement agencies in order to retrieve a lawfully installed surveillance device in 2018-19, an increase from the 20 issued in 2017-18.
- The number of tracking device authorisations increased from 54 to 210, and the number of tracking device retrieval authorisations decreased from one to zero during the reporting period. This increase is attributable to the AFP who authorised the use of tracking devices 174 times, an increase on the 25 authorisations made in 2017-18.
- Law enforcement agencies were issued eight computer access warrants in the time these powers were available during the reporting period (9 December 2018 – 30 June 2019). One application for a computer access warrant was refused by the nominated AAT member.

Table 1 illustrates the role information obtained under the Act has played in leading to arrests, safe recoveries, prosecutions, and convictions. In 2018–19, information obtained under the Act contributed to 175 arrests, 132 prosecutions, and 64 convictions.

Table 1: Number of arrests, safe recovery of a child, prosecutions, and convictions – paragraphs 50(1)(g), 50(1)(h) and 50(1)(i)

| Agency | Arrests | | Safe Recovery | | Prosecutions | | Convictions | |
|--------------|------------|------------|---------------|----------|--------------|------------|-------------|-----------|
| | 17/18 | 18/19 | 17/18 | 18/19 | 17/18 | 18/19 | 17/18 | 18/19 |
| ACIC | 53 | 46 | - | - | 6 | 5 | 6 | 5 |
| ACLEI | 1 | 1 | - | - | 2 | 4 | 1 | 1 |
| AFP | 119 | 123 | 2 | - | 101 | 122 | 30 | 57 |
| NSW Police | - | 2 | - | - | - | - | - | 1 |
| VIC Police | - | 3 | - | - | - | 1 | - | - |
| TOTAL | 173 | 175 | 2 | - | 109 | 132 | 37 | 64 |

CHAPTER ONE – WARRANTS AND OVERSIGHT

Part 2 of the Act allows law enforcement agencies to apply for three types of warrant:

- a surveillance device warrant;
- a retrieval warrant;
- a computer access warrant.

Further information on these warrants including statistics pursuant to their use during the 2018–19 reporting period can be found in chapters two, three and four.

The Act provides that an eligible Judge or nominated Administrative Appeals Tribunal (AAT) member may issue a warrant. An ‘eligible’ judge is a Judge who has consented in writing and been declared by the Minister to be an eligible Judge. During the reporting period eligible Judges included members of the:

- Family Court of Australia,
- Federal Court of Australia, and
- Federal Circuit Court of Australia.

A ‘nominated AAT member’ refers to a Deputy President, senior member, or member of the AAT who has been nominated by the Minister to issue warrants.

In the case of part-time senior members and members of the AAT, the member must have been enrolled as a legal practitioner of the High Court, another federal court, or Supreme Court of a state or the Australian Capital Territory for no less than five years to be eligible for nomination to issue warrants.

The total number of eligible Judges and nominated AAT members available to issue warrants under the Act in the reporting period is presented in Table 2.

Table 2: Availability of Federal Court Judges, Family Court Judges, Federal Circuit Court Judges, and nominated AAT members to issue warrants.

| Issuer | Number eligible | | |
|------------------------------|-----------------|-------|-------|
| | 16/17 | 17/18 | 18/19 |
| Nominated AAT Members | 31 | 39 | 33 |
| Family Court Judges | 5 | 7 | 9 |
| Federal Circuit Court Judges | 33 | 30 | 36 |
| Federal Court Judges | 13 | 14 | 15 |
| TOTAL | 82 | 90 | 93 |

Form of warrants

Generally, an application for a warrant must be in writing and be accompanied by an affidavit setting out the ground on which the warrant is sought. However, where a law enforcement officer believes that it is impractical for an application for a warrant to be made in person, applications may be made by telephone, fax, email or any other means of communication.

In urgent circumstances a law enforcement officer may make an application for a warrant before making or swearing the supporting affidavit. The law enforcement officer must supply the eligible Judge or nominated AAT member with as much information as the eligible Judge or nominated AAT member considers is reasonably practical in the circumstances. The law enforcement officer must then supply the eligible Judge or nominated AAT member with an affidavit within 72 hours of the application being made, irrespective of whether the eligible judge or nominated AAT member issues the warrant.

A warrant takes effect when it is issued and expires on a specified date, being no more than 90 days from the date the warrant is issued (or 21 days, in the case of a warrant issued for the purposes of an integrity operation), unless the warrant is revoked earlier or extended. A warrant may be extended or varied by an eligible Judge or nominated AAT member if he or she is satisfied that the grounds on which the warrant was issued still exist.

Thresholds to obtain warrants

A law enforcement agency may apply for a warrant under the Act to assist in the investigation of a 'relevant offence' which is defined as including:

- a Commonwealth offence which carries a maximum penalty of at least three years imprisonment
- state offences with a federal aspect which carry a maximum penalty of at least three years imprisonment.¹
- defined additional offences in the:
 - *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*
 - *Financial Transaction Reports Act 1988*
 - *Fisheries Management Act 1991*
 - *Torres Strait Fisheries Act 1984*
- Offences against laws of the Commonwealth, states and territories arising from integrity operations which carry a maximum penalty of at least 12 months imprisonment, or
- An offence that is prescribed by the regulations.

¹ If an application for a warrant is being made by, or on behalf of, a State or Territory law enforcement officer, a relevant offence does not include state offences that have a federal aspect.

The additional offences specified above do not carry maximum penalties of at least three years imprisonment but either:

- carry pecuniary penalties that are the equivalent of imprisonment terms of at least three years; or
- are often indicative of more serious criminal conduct.

The surveillance powers in the Act are also available to assist in the safe recovery of a child who is subject to an order made under section 67U of the *Family Law Act 1975*, or an order for a warrant for the apprehension or detention of a child under the *Family Law (Child Abduction Convention) Regulations 1986*.

Extraterritorial operation of warrants

Part 5 of the Act allows for Commonwealth law enforcement to use surveillance devices or access data held in a computer in the investigation of 'relevant offences' where the surveillance or access to the computer occurs outside Australia. With the exception of the investigation of certain offences in Australia's contiguous and fishing zones:

- the consent of an appropriate official of the foreign country must be obtained, or
- if surveillance or access to data is occurring on a vessel or aircraft, consent must be obtained from the country of registration of the vessel or aircraft.

Use of the information obtained

The Act establishes a strict regime to regulate the use, communication, and disclosure of information obtained under the Act. As a general rule, all information obtained under the Act and all information relating to the existence of a warrant or authorisation is 'protected information' and may only be used for the purposes set out in the Act. These purposes include:

- the investigation and prosecution of relevant offences, including but not limited to the offence for which surveillance powers in the Act were originally used;
- information sharing with national security agencies (ASIO, ASIS, AGO and ASD);
- disciplinary proceedings for public officers;
- the provision of international assistance to other countries, the International Criminal Court, or war crimes tribunals and
- use or communication is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property including protecting the public from a terrorist act.

Accountability provisions

The Act includes a reporting and inspection regime which allows the Commonwealth Ombudsman, the Minister, and the Parliament to scrutinise the exercise of powers under the Act.

All law enforcement agencies using the Act are required to maintain a record relating to the use of powers in the Act, and the use of information obtained through the use of powers in the Act. All law enforcement agencies must maintain a register of warrants and authorisations recording details of all warrants and authorisations and must provide a report on each warrant or authorisation issued under the Act to the Minister.

Inspections and reports by the Ombudsman

The Commonwealth Ombudsman is required to inspect the records of law enforcement agencies to ensure compliance with the Act. The Ombudsman must make a written report to the Minister at six monthly intervals on the results of each inspection. The Minister must cause a copy the report to be laid before each House of the Parliament within 15 sitting days of that House after the Minister receives it.

The Ombudsman's inspection report for the period 1 July 2018 – 31 December 2018 was laid before each House of the Parliament on 9 September 2019.

As the Ombudsman inspects agency records retrospectively, the reports detailing the Ombudsman's inspections on agency compliance with the Act for the period 1 January 2019 to 30 June 2019 have not been laid before each House of the Parliament at the time this report was provided to the Minister.

Once laid before each House of the Parliament, these reports are available at <www.ombudsman.gov.au>

CHAPTER TWO – SURVEILLANCE DEVICES

Applications for surveillance device warrants

Section 14 of the Act provides that a law enforcement officer (or another person on the officer's behalf) may apply for a surveillance device warrant for the investigation of a 'relevant offence'. The use of surveillance devices must be necessary, in the course of an investigation, for the purpose of enabling evidence to be obtained of the commission of that 'relevant offence', or the identity or location of the offenders.

Surveillance device warrants may be issued in respect of a single surveillance device, in respect of more than one kind of surveillance device, or in respect of more than one surveillance device of any particular kind. The types of surveillance devices available to law enforcement under the Act are:

- **data surveillance devices**, including any device or program used to record or monitor the input into or out of a computer.
- **listening devices**, including any device capable of being used to hear, record, monitor, or listen to conversations or words spoken but does not include a hearing aid or similar device.
- **optical surveillance devices**, including any device used to record visually or observe activity but does not include spectacles, contact lenses, or similar devices.
- **tracking devices**, meaning any electronic device capable of determining or monitoring the location of a person or an object or the status of an object.

Paragraph 50(1)(a) and paragraph 50(1)(e) of the Act provide that this report must set out the number of applications for surveillance device warrants made, issued, and refused (including reasons for any refusal) during the reporting period. Subsection 50(2) further requires that the report set out a breakdown of these numbers in respect of each different kind of surveillance device.

This information is presented in Table 3. In 2018–19 law enforcement agencies were issued 740 surveillance device warrants. Six applications for surveillance device warrants were refused by a nominated AAT member. The AFP advised their applications for surveillance device warrants were refused due to insufficient information or justification in the affidavit for the nominated AAT member to approve the warrants.

Previous annual reports included retrieval warrants as part of this table. In this annual report, information regarding retrieval warrants has been separated out and included in Table 6. As a consequence, historical information in Table 3 relating to the number of surveillance device warrants issued excludes retrieval warrants issued in those years.

Table 3: Number of surveillance device warrant applications made, issued and refused – paragraphs 50(1)(a) and 50(1)(e)

| Agency | | Composite Multiple | | | Optical | | | Listening | | | Data | | | Tracking | | | TOTAL | | |
|------------|---------|--------------------|-------|-------|---------|-------|-------|-----------|-------|-------|-------|-------|-------|----------|-------|-------|-------|-------|-------|
| | | 16/17 | 17/18 | 18/19 | 16/17 | 17/18 | 18/19 | 16/17 | 17/18 | 18/19 | 16/17 | 17/18 | 18/19 | 16/17 | 17/18 | 18/19 | 16/17 | 17/18 | 18/19 |
| ACIC | Made | 287 | 174 | 173 | - | - | - | 4 | 5 | 3 | - | 2 | 2 | 2 | 2 | - | 293 | 183 | 178 |
| | Refused | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | Issued | 287 | 174 | 173 | - | - | - | 4 | 5 | 3 | - | 2 | 2 | 2 | 2 | - | 293 | 183 | 178 |
| ACLEI | Made | 26 | 13 | 3 | - | - | - | - | - | - | - | - | - | - | - | - | 26 | 13 | 3 |
| | Refused | - | 2 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 2 | - |
| | Issued | 26 | 11 | 3 | - | - | - | - | - | - | - | - | - | - | - | - | 26 | 11 | 3 |
| AFP | Made | 732 | 580 | 551 | 1 | - | - | 4 | - | - | 2 | - | 4 | 3 | - | - | 742 | 580 | 555 |
| | Refused | - | 1 | 6 | - | - | - | - | - | - | - | - | - | - | - | - | - | 1 | 6 |
| | Issued | 732 | 579 | 545 | 1 | - | - | 4 | - | - | 2 | - | 4 | 3 | - | - | 742 | 579 | 549 |
| NSW Police | Made | 4 | 1 | 4 | - | - | - | - | - | - | - | - | - | - | - | - | 4 | 1 | 4 |
| | Refused | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | Issued | 4 | 1 | 4 | - | - | - | - | - | - | - | - | - | - | - | - | 4 | 1 | 4 |
| SA Police | Made | 1 | - | 2 | - | - | - | - | - | - | - | - | - | - | - | - | 1 | - | 2 |
| | Refused | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | Issued | 1 | - | 2 | - | - | - | - | - | - | - | - | - | - | - | - | 1 | - | 2 |
| VIC Police | Made | 3 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 3 | - | - |
| | Refused | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | Issued | 3 | - | - | - | - | - | - | - | - | - | - | - | - | - | - | 3 | - | - |
| WA Police | Made | 1 | - | 1 | - | - | - | - | 1 | 2 | - | 7 | - | - | - | 1 | 1 | 8 | 4 |
| | Refused | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - | - |
| | Issued | 1 | - | 1 | - | - | - | - | 1 | 2 | - | 7 | - | - | - | 1 | 1 | 8 | 4 |
| TOTAL | Made | 1,054 | 768 | 734 | 1 | - | - | 8 | 6 | 5 | 2 | 9 | 6 | 5 | 2 | 1 | 1,070 | 785 | 746 |
| | Refused | - | 3 | 6 | - | - | - | - | - | - | - | - | - | - | - | - | - | 3 | 6 |
| | Issued | 1,054 | 768 | 728 | 1 | - | - | 8 | 6 | 5 | 2 | 9 | 6 | 5 | 2 | 1 | 1,070 | 782 | 740 |

Remote applications for surveillance device warrants

Section 15 of the Act permits an application for a surveillance device warrant to be made by telephone, fax, email, or other means of communication if the law enforcement officer believes that it is impracticable to make the application in person. Paragraph 50(1)(d) of the Act provides that this report must set out the number of remote applications for surveillance device warrants during the reporting period.

This information is presented in Table 4. In 2018–19, there were three remote applications granted for surveillance device warrants. This represents a decrease from the nine applications granted in 2017–18.

Table 4: Number of remote applications for a surveillance device warrant – paragraph 50(1)(f)

| Agency | | Remote applications | | |
|--------|---------|---------------------|-------|-------|
| | | 16/17 | 17/18 | 18/19 |
| ACIC | Made | - | - | 3 |
| | Refused | - | - | - |
| | Granted | - | - | 3 |
| AFP | Made | 1 | 9 | - |
| | Refused | - | - | - |
| | Granted | 1 | 9 | - |
| TOTAL | Made | 1 | 9 | 3 |
| | Refused | - | - | - |
| | Granted | 1 | 9 | 3 |

Extension applications for surveillance device warrants

Section 19 of the Act provides that the law enforcement officer to whom a warrant was issued (or another person on the officer's behalf) may apply for an extension of the warrant for a period not exceeding 90 days after the warrant's original expiry date (or 21 days, in the case of a warrant issued for the purposes of an integrity operation). This application may be made at any time before the warrant expires.

Paragraph 50(1)(f) of the Act provides that the annual report must set out the number of applications for the extension of a surveillance device warrant that were made, granted, and refused (including reasons why applications were granted or refused) during the reporting period.

This information is presented in Table 4. In 2018–19 there were 234 extensions of surveillance device warrants granted to law enforcement agencies, an increase of 47 on the 187 extensions granted in 2017–18.

Table 5: Number of applications for extension of a surveillance device warrant – paragraph 50(1)(f)

| Agency | | Applications | | |
|------------|---------|--------------|-------|-------|
| | | 16/17 | 17/18 | 18/19 |
| ACIC | Made | 66 | 24 | 42 |
| | Refused | - | - | - |
| | Granted | 66 | 24 | 42 |
| ACLEI | Made | 25 | 15 | 8 |
| | Refused | - | - | - |
| | Granted | 25 | 15 | 8 |
| AFP | Made | 131 | 147 | 183 |
| | Refused | - | - | - |
| | Granted | 131 | 147 | 183 |
| NSW Police | Made | 1 | 1 | 1 |
| | Refused | - | - | - |
| | Granted | 1 | 1 | 1 |
| SA Police | Made | 2 | - | - |
| | Refused | - | - | - |
| | Granted | 2 | - | - |
| TOTAL | Made | 225 | 187 | 234 |
| | Refused | 0 | 0 | - |
| | Granted | 225 | 187 | 234 |

The ACIC advised they were granted extensions of surveillance devices warrants as their investigations are often complex and involve significant serious and organised crime which requires the collection of evidence over a sustained period. The extension of surveillance device warrants were therefore required:

- due to continuation of the operation/investigation;
- to allow the continued use of the surveillance devices;
- when insufficient evidence had been gathered up to the point prior to extension; and when
- relevant offences within the meaning of the Act were likely to be committed.

The ACLEI advised they were granted extensions of surveillance device warrants to:

- identify the use of additional, currently unknown telecommunications devices;
- enable through the use of additional warrants, the monitoring of currently unknown communications with others;
- facilitate physical surveillance for the collection of evidence; and

- allow investigators to identify the modus operandi and anticipate the activities of persons of interest and others involved in criminal activities.

The AFP advised they were granted extensions of surveillance device warrants for the continued use of surveillance devices in the investigation of serious and organised criminal activity.

NSW Police advised they were granted an extension of a surveillance device warrant because the investigation involved serious organised drug trafficking over an extended period. Surveillance devices were necessary to obtain evidence of the identity and location of multiple drug syndicate members.

International assistance applications for surveillance device warrants

Subsection 14(3A) of the Act provides that a law enforcement officer (or another person on the officer's behalf) may apply for a surveillance device warrant when they are acting under the authority of an international assistance authorisation and suspect on reasonable grounds that the use of the surveillance device is necessary for the purpose of enabling evidence to be obtained of the commission of an offence or the identity or location of the offender. The Attorney-General may issue international assistance authorisations under section 15(CA) of the *Mutual Assistance in Criminal Matters Act 1987*, section 79A of the *International Criminal Court Act 2002* and section 32A of the *International War Crimes Tribunals Act 1995* if satisfied of the following:

- a foreign country, war crimes tribunal or the International Criminal Court has requested that the Attorney-General arrange for the use of a surveillance device; and
- there is an investigation or proceeding underway within their jurisdiction (if the request is being made by a foreign country, the investigation must relate to a criminal matter involving an offence against the law of that foreign country that is punishable by a maximum penalty of imprisonment for three years or more); and
- the requesting country, war crimes tribunal, or the International Criminal Court has given undertakings regarding:
 - the information obtained via the use of surveillance devices only being used for the purposes for which it is communicated to that jurisdiction;
 - the destruction of the information obtained by the surveillance device; and
 - any other matter the Attorney-General considers appropriate.

Paragraph 50(1)(aa) and paragraph 50(1)(ea) of the Act provides that this report must set out the number of surveillance device warrants pursuant to an international assistance application made, issued, and refused (including the reasons for any refusal) during the reporting period.

Where a surveillance device warrant was issued as a result of an international assistance application, paragraph 50(1)(ia) of the Act requires that this report list the offence (if any) under a law of the Commonwealth, states, or territories that is of the same or substantially similar nature as the foreign offence being investigated under that same surveillance device warrant.

In 2018–19, no law enforcement agencies applied for a surveillance device warrant as a result of an international assistance authorisation.

Applications for retrieval warrants

Section 22 of the Act provides that a law enforcement officer (or another person on the officer's behalf) may apply for a retrieval warrant in respect of a surveillance device that was lawfully installed on premises, or in or on an object, under a surveillance device warrant or a tracking device authorisation. The officer must suspect on reasonable grounds that the device is still on those premises or in or on that object, or on other premises, or in or on another object.

Paragraph 50(1)(a) and paragraph 50(1)(e) of the Act provide that this report must set out the number of applications for retrieval warrants made, issued, and refused (including reasons for any refusal) during the reporting period. Subsection 50(2) further requires that the report set out a breakdown of these numbers in respect of each different kind of surveillance device.

This information is presented in Table 6. In 2018–19 law enforcement agencies were issued 31 warrants to retrieve a surveillance device, an increase on the 20 issued in 2017–18.

Remote applications for retrieval warrants

Section 23 of the Act permits an application for a retrieval warrant to be made by telephone, fax, email, or other means of communication if the law enforcement officer believes that it is impracticable to make the application in person. Paragraph 50(1)(d) of the Act provides that this report must set out the number of remote applications for retrieval warrants during the reporting period.

In 2018–19, no remote applications for a retrieval warrant were made.

Table 6: Number of retrieval warrant applications made, issued and refused² – paragraphs 50(1)(a) and 50(1)(e)

| Agency | | Composite Multiple 18/19 | Optical 18/19 | Listening 18/19 | Data 18/19 | Tracking 18/19 | TOTAL | | |
|------------|---------|--------------------------------|------------------|--------------------|---------------|-------------------|-------|-------|-------|
| | | | | | | | 16/17 | 17/18 | 18/19 |
| ACIC | Made | - | - | - | - | 5 | 4 | 4 | 5 |
| | Refused | - | - | - | - | - | - | - | - |
| | Issued | - | - | - | - | 5 | 4 | 4 | 5 |
| ACLEI | Made | 2 | - | - | - | - | - | - | 2 |
| | Refused | - | - | - | - | - | - | - | - |
| | Issued | 2 | - | - | - | - | - | - | 2 |
| AFP | Made | 16 | - | 3 | 1 | 3 | 39 | 16 | 23 |
| | Refused | - | - | - | - | - | - | - | - |
| | Issued | 16 | - | 3 | 1 | 3 | 39 | 16 | 23 |
| NSW Police | Made | 1 | - | - | - | - | - | - | 1 |
| | Refused | - | - | - | - | - | - | - | - |
| | Issued | 1 | - | - | - | - | - | - | 1 |
| TOTAL | Made | 19 | - | 3 | 1 | 8 | 43 | 20 | 31 |
| | Refused | - | - | - | - | - | - | - | - |
| | Issued | 19 | - | 3 | 1 | 8 | 43 | 20 | 31 |

² In previous years, agencies were not asked to list the kinds of surveillance devices retrieved under retrieval warrants. To improve the information presented in the annual report, agencies have been asked to provide this information from the 2018-19 reporting period onwards.

Use of surveillance devices without a warrant – emergency circumstances

In special circumstances, an appropriate authorising officer of a law enforcement agency may issue an emergency authorisation enabling the use of surveillance devices or to access data held in a computer, without a warrant. An emergency authorisation may only be issued in urgent circumstances when:

- there is an imminent risk of serious violence to a person or substantial damage to property (section 28),
- it is necessary to assist in the recovery of a child who is subject to a recovery order (section 29), or
- there is a risk of loss of evidence for certain serious offences such as drug offences, terrorism, espionage, sexual servitude, and aggravated people smuggling (section 30).

The use of surveillance under such an authorisation must be retrospectively approved by an eligible Judge or AAT member within 48 hours of the authorisation being issued.

Paragraph 50(1)(b) and paragraph 50(1)(e) provides that this report must set out the number of applications for emergency authorisations made, given, and refused (including the reasons for any refusal) during the reporting period). Subsection 50(2) further requires that the report set out a breakdown of these numbers in respect of each different kind of surveillance device.

In 2018–19, the AFP applied for, and were issued, one emergency authorisation to use a tracking device without a warrant. No other agencies made emergency authorisations.

Use of surveillance devices without a warrant – investigative purposes

Optical surveillance devices may be used by a law enforcement officer without a warrant where the device can be installed and retrieved without either entering premises or interfering with a vehicle or thing without permission.

In limited circumstances, listening devices may be used without a warrant by a law enforcement officer who is a party to the conversation being recorded or is included in a class or group of persons whom the speaker of the words intends will, or should reasonably expect would, hear the conversation.

Tracking device authorisations

In limited circumstances, section 39 of the Act permits a law enforcement officer to use a tracking device without a warrant in the investigation of a relevant offence or to assist in the location and safe recovery of a child to whom a recovery order relates where the officer has the written permission of an appropriate authorising officer.

An authorisation made under this provision is subject to subsection 39(8) of the Act which states that a tracking device cannot be used, installed, or retrieved if it involves entry onto premises or an interference with the interior of a vehicle without permission. The permission may come from the owner, occupier, or under a surveillance device warrant. Where such use requires a greater level of intrusion (such as entry onto premises without permission), a surveillance device warrant is required.

Paragraph 50(1)(c) and paragraph 50(1)(e) provide that this report must set out the number of applications for tracking device authorisations made, given, and refused (including reasons for any refusal) during the reporting period. This includes the number of tracking device retrievals, which may be authorised without a warrant in accordance with subsection 39(6) of the Act.

This information is presented in Table 7. In 2018–19, law enforcement agencies applied for 210 tracking device authorisations, an increase of 156 on the 54 given in 2017–18. No law enforcement agencies applied for a tracking device retrieval authorisation in 2018–19.

Table 7: Number of applications for tracking device authorisations – paragraphs – 50(1)(c) and 50(1)(e)

| Agency | | Tracking Device Authorisations | | | Tracking Device Retrievals | | |
|------------|---------|--------------------------------|-------|-------|----------------------------|-------|-------|
| | | 16/17 | 17/18 | 18/19 | 16/17 | 17/18 | 18/19 |
| ACIC | Made | 20 | 29 | 35 | - | - | - |
| | Refused | - | - | - | - | - | - |
| | Issued | 20 | 29 | 35 | - | - | - |
| AFP | Made | 29 | 25 | 174 | - | 1 | - |
| | Refused | - | - | - | - | - | - |
| | Issued | 29 | 25 | 174 | - | 1 | - |
| SA Police | Made | 1 | - | - | - | - | - |
| | Refused | - | - | - | - | - | - |
| | Issued | 1 | - | - | - | - | - |
| VIC Police | Made | - | - | 1 | - | - | - |
| | Refused | - | - | - | - | - | - |
| | Issued | - | - | 1 | - | - | - |
| TOTAL | Made | 50 | 54 | 210 | - | 1 | - |
| | Refused | - | - | - | - | - | - |
| | Issued | 50 | 54 | 210 | - | 1 | - |

CHAPTER THREE – COMPUTER ACCESS WARRANTS

Computer access warrants were introduced to the Act by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* following its royal assent on 8 December 2018. The computer access warrant statistics in this chapter reflect their availability to law enforcement agencies during the reporting period, between 9 December 2018 and 30 June 2019.

Applications for computer access warrants

Section 27A of the Act provides that a law enforcement officer (or another person on the officer's behalf) may apply for the issue of a computer access warrant for the investigation of a 'relevant offence', which generally carry a maximum imprisonment term of at least three years. Access to data held in a computer must be necessary, in the course of an investigation, for the purpose of enabling evidence to be obtained of the commission of that 'relevant offence', or the identity or location of the offenders.

A computer access warrant must specify the things that are authorised under the warrant, which may include:

- entering premises for the purposes of executing the warrant;
- using the target computer, a telecommunications facility, electronic equipment or data storage device in order to access data held in the target computer to determine whether it is relevant data and is covered by the warrant;
- adding, copying, deleting or altering data in the target computer if necessary to access the data to determine whether it is relevant and covered by the warrant;
- using any other computer if necessary to access the data (and adding, copying, deleting or altering data on that computer if necessary);
- removing a computer from premises for the purposes of executing the warrant;
- copying data to which access has been obtained that is relevant and covered by the warrant;
- intercepting a communication in order to execute the warrant; and
- any other thing reasonably incidental to the above things.

Computer access warrants do not authorise the addition, deletion or alteration of data, or the doing of anything that is likely to materially interfere with, interrupt or obstruct a communication in transit or the lawful use by other persons of a computer, unless it is necessary to do one or more of the things specified in a warrant. Except where necessary for concealment, computer access warrants do not authorise any other material loss or damage to other persons lawfully using a computer.

Paragraph 50(1)(a) and paragraph 50(1)(e) of the Act provide that this report must set out the number of applications for computer access warrants made, issued, and refused (including reasons for any refusal) during the reporting period.

Section 27B of the Act permits a remote application for a computer access warrant to be made by telephone, fax, email, or other means of communication if the law enforcement officer believes that it is impracticable to make the application in person. Paragraph 50(1)(d) of the Act provides that this report must set out the number of remote applications during the reporting period.

Section 27F of the Act provides that the law enforcement officer to whom a computer access warrant was issued (or another person on the officer's behalf) may apply for an extension of the warrant for a period not exceeding 90 days after the warrant's original expiry date (or 21 days, in the case of a warrant issued for the purposes of an integrity operation). This application may be made at any time before the warrant expires.

Paragraph 50(1)(f) of the Act provides that the annual report must set out the number of applications for the extension of a computer access warrant that were made, granted, and refused (including reasons why applications were granted or refused) during the reporting period.

This information is presented in Table 8. In 2018–19, law enforcement agencies were issued eight computer access warrants. The ACIC applied for, and were issued one computer access warrant. The AFP were issued seven computer access warrants, with one refused by a nominated AAT member. The AFP reported the warrant was refused due to concerns raised by an AAT member that a physical computer had to be identified. The AFP also applied for, and were issued, two extensions of computer access warrants. The AFP advised these extensions were granted due to ongoing investigations.

No agencies made remote applications for computer access warrants during 2018–19.

Table 8: Number of computer access warrants issued, remote applications made, and extensions granted between 9 December 2018 and 30 June 2019 – paragraphs 50(1)(a), 50(1)(d), 50(1)(e) and 50(1)(f)

| Agency | | Applications for 2018 / 19 | | |
|--------|---------|----------------------------|---------------------|------------------------|
| | | Warrant Applications | Remote Applications | Extensions of Warrants |
| ACIC | Made | 1 | - | - |
| | Refused | - | - | - |
| | Issued | 1 | - | - |
| AFP | Made | 8 | - | 2 |
| | Refused | 1 | - | - |
| | Issued | 7 | - | 2 |
| TOTAL | Made | 9 | - | 2 |
| | Refused | 1 | - | - |
| | Issued | 8 | - | 2 |

International assistance applications for computer access warrants

Subsection 27A(4) of the Act provides that a law enforcement officer (or another person on the officer's behalf) may apply for a computer access warrant when they are acting under the authority of an international assistance authorisation and the law enforcement officer suspects on reasonable grounds that access to data held in a computer is necessary for the purpose of enabling evidence to be obtained of the commission of an offence or the identity or location of the offender. The Attorney-General may issue international assistance authorisations under section 15(CC) of the *Mutual Assistance in Criminal Matters Act 1987*, section 79B of the *International Criminal Court Act 2002* and section 32AA of the *International War Crimes Tribunals Act 1995* if satisfied of the following:

- a foreign country, war crimes tribunal, or the International Criminal Court has requested that the Attorney-General arrange for access to data held on a computer; and
- there is an investigation or proceeding underway within their jurisdiction (if the request is being made by a foreign country, the investigation must relate to a criminal matter involving an offence against the law of that foreign country that is punishable by a maximum penalty of imprisonment for three years or more); and
- the requesting foreign country, war crimes tribunal, or the International Criminal Court has given undertakings regarding:
 - the information obtained via a computer access warrant only being used for the purposes for which it is communicated to the jurisdiction;
 - the destruction of the information obtained under the computer access warrant; and
 - any other matter the Attorney-General considers appropriate.

Paragraph 50(1)(aa) and paragraph 50(1)(ea) of the Act provide that this report must set out the number of warrants pursuant to an international assistance application made, issued, and refused (including the reasons for any refusal) during the reporting period.

Where a computer access warrant was issued as a result of an international assistance application, paragraph 50(1)(ia) of the Act requires that this report list the offence (if any) under a law of the Commonwealth, states, or territories that is of the same or substantially similar nature as the foreign offence being investigated under that same computer access warrant.

In 2018–19, no law enforcement agencies applied for a computer access warrant as a result of an international assistance application.

CHAPTER FOUR – EFFECTIVENESS OF THE ACT

Paragraph 50(1)(g) provides that this report must set out the number of arrests made, wholly or partly, on the basis of information obtained under a warrant, an emergency authorisation, or a tracking device authorisation. Paragraph 50(1)(i) requires that this report set out the number of prosecutions commenced in which information obtained under a warrant, emergency authorisation, or tracking device authorisation was given in evidence and the number of prosecutions in which a person was found guilty (convictions). Paragraph 50(1)(h) provides that this report must set out the number of instances in which the location and safe recovery of a child, to whom a recovery order related, was assisted, wholly or partly, on the basis of information obtained under a warrant, emergency authorisation, or tracking device authorisation.

Collectively, this information provides an indication of the effectiveness of the use of surveillance powers in the Act as a law enforcement investigative tool.

This information is presented in Table 9. In 2018–19, information obtained under the Act contributed to 175 arrests, 132 prosecutions, and 64 convictions.

Table 9: Number of arrests, safe recovery, prosecutions, and convictions – paragraphs 50(1)(g), 50(1)(h) and 50(1)(i)

| Agency | Arrests | | Safe Recovery | | Prosecutions | | Convictions | |
|--------------|------------|------------|---------------|----------|--------------|------------|-------------|-----------|
| | 17/18 | 18/19 | 17/18 | 18/19 | 17/18 | 18/19 | 17/18 | 18/19 |
| ACIC | 53 | 46 | - | - | 6 | 5 | 6 | 5 |
| ACLEI | 1 | 1 | - | - | 2 | 4 | 1 | 1 |
| AFP | 119 | 123 | 2 | - | 101 | 122 | 30 | 57 |
| NSW Police | - | 2 | - | - | - | - | - | 1 |
| VIC Police | - | 3 | - | - | - | 1 | - | - |
| TOTAL | 173 | 175 | 2 | - | 109 | 132 | 37 | 64 |

Interpretive note

The information presented in Table 9 should be interpreted with caution, particularly presuming a relationship between the number of arrests, prosecutions (which include committal proceedings), and convictions in a reporting period. An arrest recorded in one reporting period may not result in a prosecution or committal (if at all) until a later reporting period. Moreover, the number of arrests may not equate to the number of charges laid (some or all of which may be prosecuted at a later time) as an arrested person may be prosecuted and convicted for a number of offences.

Further, the table may understate the effectiveness of the Act as, in some cases, prosecutions may be initiated and convictions recorded without the need to give information obtained under the Act in evidence. In particular, agencies report that the

use of the Act effectively enables investigators to identify persons involved in, and the infrastructure of, organised criminal activities. In many cases, the weight of evidence obtained through the use of the Act results in defendants entering guilty pleas, thereby removing the need for the information to be introduced into evidence.

CHAPTER FIVE – FURTHER INFORMATION

Further information about the *Surveillance Devices Act 2004* can be obtained by contacting the Department of Home Affairs:

National Security Policy Branch

Department of Home Affairs

PO Box 25

Belconnen ACT 2616

Telephone: (02) 6264 1111

Previous *Surveillance Devices Act 2004* Annual Reports can be accessed online at:
<www.homeaffairs.gov.au>

APPENDIX A – LIST OF TABLES

| Table | Heading | Page # |
|-----------------|---|--------|
| TABLE 1: | Number of arrests, safe recovery, prosecutions, and convictions – paragraphs 50(1)(g), 50(1)(h) and 50(1)(i) | 3 |
| TABLE 2: | Availability of Federal Court Judges, Family Court Judges, Federal Circuit Court Judges, and nominated AAT members to issue warrants | 4 |
| TABLE 3: | Number of surveillance device warrants issued – paragraphs 50(1)(a) and 50(1)(e) | 9 |
| TABLE 4: | Number of remote applications for a surveillance device warrant – paragraphs 50(1)(a) and 50(1)(e) | 10 |
| TABLE 5: | Number of applications for extension of a surveillance device warrant – paragraph 50(1)(f) | 11 |
| TABLE 6: | Number of retrieval warrants issued – paragraphs 50(1)(a) and 50(1)(e) | 14 |
| TABLE 7: | Number of applications for tracking device authorisations – paragraphs 50(1)(c) and 50(1)(e) | 17 |
| TABLE 8: | Number of computer access warrants issued, remote applications made, and extensions granted between 9 December 2018 and 30 June 2019 – paragraphs 50(1)(a), 50(1)(d), 50(1)(e) and 50(1)(f) | 19 |
| TABLE 9: | Number of arrests, safe recovery, prosecutions, and convictions – paragraphs 50(1)(g), 50(1)(h) and 50(1)(i) | 21 |

APPENDIX B – ABBREVIATIONS

| Abbreviation | Name |
|-------------------|---|
| AAT | Administrative Appeals Tribunal |
| ACIC | Australian Criminal Intelligence Commission |
| ACLEI | Australian Commission for Law Enforcement Integrity |
| Act | Surveillance Devices Act 2004 |
| AFP | Australian Federal Police |
| AGO | Australian Geospatial-Intelligence Organisation |
| ASD | Australian Signals Directorate |
| ASIO | Australian Security Intelligence Organisation |
| ASIS | Australian Secret Intelligence Service |
| CCC (WA) | Corruption and Crime Commission (Western Australia) |
| CCC (QLD) | Crime and Corruption Commission (Queensland) |
| IBAC | Independent Broad-based Anti-corruption Commission (Victoria) |
| ICAC (NSW) | Independent Commission Against Corruption (New South Wales) |
| ICAC (SA) | Independent Commissioner Against Corruption (South Australia) |
| LECC | Law Enforcement Conduct Commission |
| NSW CC | New South Wales Crime Commission |
| NSW Police | New South Wales Police |
| NT Police | Northern Territory Police |
| QLD Police | Queensland Police |
| SA Police | South Australia Police |
| TAS Police | Tasmania Police |
| VIC Police | Victoria Police |
| WA Police | Western Australia Police |

NOTES

This image shows a single page of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page, leaving small margins at the top and bottom. There are no vertical margin lines, text, or other markings on the page.

