Australian Government
Department of Home Affairs

Surveillance Devices Act 2004
Annual Report 2020-21

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

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

Surveillance Devices Act 2004

Annual Report 2020–21

Contents

EXECUTIVE SUMMARY

The *Surveillance Devices Act 2004* (the SD 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 SD Act. The Annual Report for 2020–21 describes the extent and circumstances in which eligible Commonwealth, State and Territory law enforcement agencies have used the powers available under the SD Act between 1 July 2020 and 30 June 2021.

Objects of the SD Act

The SD Act provides a legislative regime for Commonwealth agencies to use surveillance devices and access data held in computers.

The SD Act also authorises State and Territory law enforcement agencies to use surveillance devices and access data held in computers for certain investigations relevant to Commonwealth offences.

The SD Act also restricts the use, communication, and publication of information that is obtained through the use of powers under the SD Act.

Powers under the SD 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
- Corruption and Crime Commission of Western Australia
- Independent Broad-based Anti-corruption Commission of Victoria
- Independent Commission Against Corruption of New South Wales
- Independent Commissioner Against Corruption of South Australia
- New South Wales Crime Commission
- New South Wales Law Enforcement Conduct Commission (LECC)

Information relating to the administration of the SD Act

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

Legislative reforms

Surveillance Legislation Amendment (Identify and Disrupt) Act 2021

The Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 was introduced into the House of Representatives on 3 December 2020 and was referred to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for review on 8 December 2020.

The Bill provides the Australian Federal Police (AFP) and Australian Criminal Intelligence Commission (ACIC) with new powers to identify and disrupt serious criminal activities online, including to introduce data disruption warrants and network activity warrants into the SD Act. Data disruption warrants enable the AFP and the ACIC to frustrate the commission of serious offences online by modifying, adding, copying or deleting data. Network activity warrants enable the AFP and ACIC to collect intelligence on serious criminal activity carried out by criminal networks online. The Bill also introduces account takeover warrants into the *Crimes Act 1914* to allow the AFP and ACIC to take control of a person's online account to gather evidence about criminal activity.

After the end of the report period, but before the publication of this report, the PJCIS handed down its report on the SLAID Bill on 5 August 2021. A copy of this report is available here: <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IdentifyandDisruptBill/Report>. The majority of the PJCIS's recommendations were implemented through parliamentary debate and the Bill passed Parliament on 25 August 2021, with the new powers commencing on 4 September 2021.

Policy developments

There were three separate reviews, either commenced, completed or published in 2020-21, which may result in future legislative reforms to the SD Act.

Comprehensive review of the legal framework governing the National Intelligence Community

The current electronic surveillance legislative framework was examined extensively in the Comprehensive Review of the Legal Framework of the National Intelligence Community (the Comprehensive Review). The Comprehensive Review identified that the current laws are complex, inconsistent, outdated and inflexible. Frequent amendments are needed to keep pace with technological change and the evolving criminal and national security threats resulting in a patchwork of overlapping and at times inconsistent, incompatible or contradictory parts. This puts at risk the effectiveness of protections for people's information and data, and the proper governance of agencies who access this information. It also creates difficulties for agencies when investigating serious criminality and threats to national security.

In its response, the Government committed to reform the existing laws and develop a new Act that is clearer, more coherent and better adapted to the modern world. On 1 July 2021, the Department of Home Affairs established an interagency taskforce to deliver on the Government's commitment. This will involve repealing and replacing

the powers currently divided between the SD Act, the *Telecommunications (Interception and Access) Act 1979* and parts of the *Australian Security Intelligence Organisation Act 1979* into one consolidated Act.

The development of a new electronic surveillance legislative framework will require detailed consideration, informed by extensive consultation with Commonwealth, State and Territory government agencies, international partners, industry, and civil society groups. The Government intends to develop a new modernised and streamlined electronic surveillance legislative framework by 2023.

The Government will conduct open and iterative public consultation throughout the development of the new framework.

Independent National Security Legislation Monitor review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

In July 2020, the then Independent National Security Legislation Monitor (INSLM), Dr James Renwick CSC SC, handed down his report concerning the new framework introduced by the *Telecommunications and Other Legislation (Assistance and Access) Act 2018* (the Assistance and Access Act). The Assistance and Access Act introduced industry assistance measures in the *Telecommunications Act 1997* and computer access warrants in the SD Act to better deal with the challenges posed by ubiquitous encryption. The INSLM was asked to consider whether the amendments introduced by the Assistance and Access Act contains appropriate safeguards for protecting the rights of individuals, and remains proportionate to the threats against national security and necessary.

The INSLM concluded that the amendments introduced by the Assistance and Access Act are necessary and proportionate, subject to some amendments that were recommended. The INSLM made 33 recommendations, including three in relation to computer access warrants in the SD Act.

The INSLM report has been provided to the PJCIS to inform its current review of the Assistance and Access Act. The Department of Home Affairs made a submission to the PJCIS review which provided commentary on the INSLM's recommendations. The Department's submission can be found here:

<https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Submissions>.

Parliamentary Joint Committee on Intelligence and Security review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018

The PJCIS is conducting its third review into the Assistance and Access Act. This review will build on both the previous two PJCIS reviews, and the INSLM review of the Assistance and Access Act.

As of September 2021, the PJCIS had not published its report. The Government will carefully consider the findings made by the INSLM and PJCIS reviews together.

For further information on these reviews including committee reports and submissions, visit:

- Comprehensive review of the legal framework of the National Intelligence Community <https://www.ag.gov.au/national-security/consultations/comprehensive-review-legal-framework-governing-national-intelligence-community>
- Independent National Security Legislation Monitor review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* <https://www.inslm.gov.au/reviews-reports/telecommunications-and-other-legislation-amendment-act-2018-related-matters>
- Parliamentary Joint Committee on Intelligence and Security review of the amendments made by the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018>

Key statistics

- In 2020–21, information obtained under the SD Act contributed to 371 arrests, 50 prosecutions, and 42 convictions.
- In 2020–21, 5 law enforcement agencies were issued 830 surveillance device warrants, an increase of 67 from the 763 issued in 2019–20. Three applications for surveillance device warrants were refused by nominated AAT members.
- 367 applications to extend surveillance device warrants were granted, a decrease of 91 from the 458 granted in 2019-20. Applications to extend warrants are often required due to the prolonged nature of investigations for complex and serious crime (where evidence gathering may not have been completed within 90 days).
- 17 retrieval warrants were issued to law enforcement agencies in order to retrieve a lawfully installed surveillance device in 2020–21, a decrease of 3 from the 20 issued in 2019–20.
- 49 tracking device authorisations were issued in 2020-21, a decrease of 51 from the 100 issued in 2019-20. One tracking device retrieval authorisation was issued, the same number as in 2019-20.
- 23 computer access warrants were issued to law enforcement agencies during 2020-21, an increase of 3 from the 20 issued in 2019-20.

CHAPTER ONE – WARRANTS AND OVERSIGHT

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

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

Further information on these warrants including statistics on their use during the 2020–21 reporting period can be found in chapters two, three and four of this report.

The SD 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 Attorney-General 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 (of any level) who has been nominated by the Attorney-General 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 SD Act in the reporting period is presented in Table 1.

Table 1: Availability of Federal Court Judges, Family Court Judges, Federal Circuit Court Judges, and nominated AAT members to issue warrants.

Issuing authority	Number		
	18/19	19/20	20/21
Nominated AAT Members	33	36	36
Family Court Judges	9	10	10
Federal Circuit Court Judges	36	32	32
Federal Court Judges	15	13	13
TOTAL	**93**	**91**	**91**

Form of warrants

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

A warrant has effect for the period specified in the warrant, which cannot exceed 90 days (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 continue to exist.

Thresholds to obtain warrants

A law enforcement agency may apply for a warrant under the SD 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]
- additional offences specified 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.

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 indicative of more serious criminal conduct.

The surveillance powers in the SD 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*,

[1] A State or Territory law enforcement officer cannot seek a warrant for State offences that have a federal aspect.

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 SD Act allows for Commonwealth law enforcement agencies to use surveillance devices or access data held in a computer in the investigation of 'relevant offences' where there is a need for surveillance, or access to data held in a computer 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.

Consent from an appropriate official is not required for a computer access warrant, if the person executing the warrant is physically present in Australia and the location where the data is held is unknown or cannot reasonably be determined.

Use of the information obtained

The SD Act restricts the use, communication, and disclosure of information obtained under the SD Act. As a general rule, all information obtained under the SD 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 SD Act. These purposes include:

- the investigation and prosecution of relevant offences, including but not limited to the offence for which surveillance powers in the SD 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 SD Act includes a reporting and inspection regime which allows the Commonwealth Ombudsman, the Minister for Home Affairs, and the Parliament to scrutinise the exercise of powers under the SD Act.

All law enforcement agencies are required to maintain records relating to each warrant or authorisation, and the use of information obtained through the use of powers in the SD 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 SD Act to the Minister for Home Affairs.

Inspections and reports by the Ombudsman

The Commonwealth Ombudsman is required to inspect the records of law enforcement agencies to ensure compliance with the SD Act. The Ombudsman must make a written report to the Minister at six monthly intervals on the results of each inspection. The Minister for Home Affairs 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 for Home Affairs receives it.

The Ombudsman's inspection report for the period 1 July 2020 – 31 December 2020 was laid before each House of the Parliament in March 2021.

As the Ombudsman inspects agency records retrospectively, the reports detailing the Ombudsman's inspections on agency compliance with the SD Act for the period 1 January 2020 to 30 June 2021 have not been laid before each House of the Parliament at the time this report was provided to the Minister for Home Affairs.

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 SD 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 SD 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.

Paragraphs 50(1)(a) and 50(1)(e) of the SD Act provide that this report must set out the number of applications for surveillance device warrants made and refused (including reasons for any refusal), and the number of warrants issued, 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 2. In 2020–21 law enforcement agencies were issued 830 surveillance device warrants. Three applications for surveillance device warrants were refused by a nominated AAT member. The AFP advised its applications for surveillance device warrants were refused due to nominated AAT members not being satisfied the affidavit contained enough information to link the subject of the warrant to the relevant offences being investigated.

Table 2: 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		
		18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21
ACIC	Made	173	126	62	-	-	-	3	1	-	2	-	1	-	4	2	**178**	**131**	**65**
	Refused	-	2	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**	**2**	**-**
	Issued	173	124	62	-	-	-	3	1	-	2	-	1	-	4	2	**178**	**129**	**65**
ACLEI	Made	3	9	4	-	-	-	-	-	-	-	-	-	-	-	-	**3**	**9**	**4**
	Refused	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**	**-**	**-**
	Issued	3	9	4	-	-	-	-	-	-	-	-	-	-	-	-	**3**	**9**	**4**
AFP	Made	551	628	744	-	-	1	-	-	4	4	-	1	-	-	1	**555**	**628**	**751**
	Refused	6	8	3	-	-	-	-	-	-	-	-	-	-	-	-	**6**	**8**	**3**
	Issued	545	620	741	-	-	1	-	-	4	4	-	1	-	-	1	**549**	**620**	**748**
LECC	Made	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	**-**	**-**	**1**
	Refused	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**	**-**	**-**
	Issued	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	**-**	**-**	**1**
NSW Police	Made	4	1	-	-	-	-	-	-	-	-	-	-	-	-	-	**4**	**1**	**-**
	Refused	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**	**-**	**-**
	Issued	4	1	-	-	-	-	-	-	-	-	-	-	-	-	-	**4**	**1**	**-**
SA Police	Made	2	4	-	-	-	-	-	-	-	-	-	-	-	-	-	**2**	**4**	**-**
	Refused	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**	**-**	**-**
	Issued	2	4	-	-	-	-	-	-	-	-	-	-	-	-	-	**2**	**4**	**-**
WA Police	Made	1	-	4	-	-	-	2	-	-	-	-	8	1	-	-	**4**	**-**	**12**
	Refused	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**	**-**	**-**
	Issued	1	-	4	-	-	-	2	-	-	-	-	8	1	-	-	**4**	**-**	**12**
TOTAL	**Made**	**734**	**768**	**814**	**-**	**-**	**1**	**5**	**1**	**4**	**6**	**-**	**10**	**1**	**4**	**4**	**746**	**773**	**833**
	Refused	**6**	**10**	**3**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**6**	**10**	**3**
	Issued	**728**	**758**	**811**	**-**	**-**	**1**	**5**	**1**	**4**	**6**	**-**	**10**	**1**	**4**	**4**	**740**	**763**	**830**

Remote applications for surveillance device warrants

Section 15 of the SD 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 SD 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 3. In 2020–21, there were no remote applications made for surveillance device warrants. This is a decrease from the two applications made in 2019–20.

Table 3: Number of remote applications for a surveillance device warrant – paragraph 50(1)(d)

Agency		Remote applications		
		18/19	19/20	20/21
ACIC	Made	3	2	-
	Refused	-	-	-
	Issued	3	2	-
AFP	Made	-	-	-
	Refused	-	-	-
	Issued	-	-	-
TOTAL	**Made**	**3**	**2**	**-**
	Refused	**-**	**-**	**-**
	Issued	**3**	**2**	**-**

Extension applications for surveillance device warrants

Section 19 of the SD 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 SD Act provides that the annual report must set out the number of applications for the extension of a surveillance device warrant that were made, and the number of extensions granted and refused (including reasons why applications were granted or refused) during the reporting period.

This information is presented in Table 4. In 2020–21 there were 367 extensions of surveillance device warrants granted to law enforcement agencies, a decrease of 91 from the 458 extensions granted in 2019–20.

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

Agency		Applications		
		18/19	19/20	20/21
ACIC	Made	42	79	29
	Refused	-	-	-
	Granted	42	79	29
ACLEI	Made	8	3	-
	Refused	-	-	-
	Granted	8	3	-
AFP	Made	183	375	338
	Refused	-	-	-
	Granted	183	375	338
NSW Police	Made	1	1	-
	Refused	-	-	-
	Granted	1	1	-
SA Police	Made	-	-	-
	Refused	-	-	-
	Granted	-	-	-
TOTAL	**Made**	**234**	**458**	**367**
	Refused	**-**	**-**	**-**
	Granted	**234**	**458**	**367**

The ACIC and the AFP advised they sought and were granted extensions of surveillance devices warrants in relation to complex investigations involving significant serious and organised crime, which requires the collection of evidence over a sustained period.

International assistance applications for surveillance device warrants

Subsection 14(3A) of the SD 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 15CA 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.

Paragraphs 50(1)(aa) and 50(1)(ea) of the SD Act provides that this report must set out the number of international assistance applications made and refused (including the reasons for any refusal), and the number of such warrants issued as a result 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 SD 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 2020–21, no law enforcement agencies applied for a surveillance device warrant as a result of an international assistance authorisation. This remains the same as 2019-20

Applications for retrieval warrants

Section 22 of the SD 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.

Paragraphs 50(1)(a) and 50(1)(e) of the SD Act provide that this report must set out the number of applications for retrieval warrants made and refused (including reasons for any refusal), and the number of warrants issued 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 5. In 2020–21 law enforcement agencies were issued 17 warrants to retrieve a surveillance device, a decrease on the 20 issued in 2019–20.

Remote applications for retrieval warrants

Section 23 of the SD 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 SD Act provides that this report must set out the number of remote applications for retrieval warrants during the reporting period.

In 2020–21, no remote applications for a retrieval warrant were made. This remains the same as 2019-20.

Table 5: Number of retrieval warrant applications made, issued and refused – paragraphs 50(1)(a) and 50(1)(e)

Agency		Composite Multiple			Optical			Listening			Data			Tracking			TOTAL		
		18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21
ACIC	Made	-	2	-	-	-	-	-	1	2	-	-	-	5	1	-	**5**	**4**	**2**
	Refused	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**	**-**	**-**
	Issued	-	2	-	-	-	-	-	1	2	-	-	-	5	1	-	**5**	**4**	**2**
ACLEI	Made	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**2**	**-**	**-**
	Refused	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**	**-**	**-**
	Issued	2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**2**	**-**	**-**
AFP	Made	16	9	8	-	-	-	3	3	2	1	-	1	3	4	4	**23**	**16**	**15**
	Refused	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**	**-**	**-**
	Issued	16	9	8	-	-	-	3	3	2	1	-	1	3	4	4	**23**	**16**	**15**
NSW Police	Made	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1**	**-**	**-**
	Refused	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**-**	**-**	**-**
	Issued	1	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**1**	**-**	**-**
TOTAL	**Made**	**19**	**11**	**8**	**-**	**-**	**-**	**3**	**4**	**4**	**1**	**-**	**1**	**8**	**5**	**4**	**31**	**20**	**17**
	Refused	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
	Issued	**19**	**11**	**8**	**-**	**-**	**-**	**3**	**4**	**4**	**1**	**-**	**1**	**8**	**5**	**4**	**31**	**20**	**17**

Use of surveillance devices in emergency circumstances

An appropriate authorising officer of a law enforcement agency may issue an emergency authorisation enabling the use of surveillance devices without a warrant. An emergency authorisation may only be issued in urgent circumstances when it is not practicable to apply for a warrant and:

- there is an imminent risk of serious violence to a person or substantial damage to property (section 28),
- a recovery order in relation to a child is in force (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.

Paragraphs 50(1)(b) and 50(1)(e) provides that this report must set out the number of applications for emergency authorisations made and refused (including the reasons for any refusal) and the number of authorisations given 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 2020–21, no law enforcement agency made an emergency authorisation for the use of surveillance devices. This remains the same as 2019-20.

Tracking device authorisations

Section 39 of the SD 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 SD 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 or occupier. Where such use requires a greater level of intrusion (such as entry onto premises without permission), a surveillance device warrant is required.

Paragraphs 50(1)(c) and 50(1)(e) provide that this report must set out the number of applications for tracking device authorisations made, and the number of such authorisations given, and the number of applications 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 SD Act.

This information is presented in Table 6. In 2020–21, law enforcement agencies made 49 tracking device authorisations, a decrease of 51 on the 100 given in 2019–20. One tracking device retrieval authorisation was given by the AFP in 2020-21, the same number as given in 2019-20.

Table 6: Number of applications for tracking device authorisations – paragraphs – 50(1)(c) and 50(1)(e)

Agency		Tracking Device Authorisations			Tracking Device Retrievals		
		18/19	**19/20**	**20/21**	**18/19**	**19/20**	**20/21**
ACIC	Made	35	25	9	-	-	-
	Refused	-	-	-	-	-	-
	Given	35	25	9	-	-	-
AFP	Made	175	74	40	-	1	1
	Refused	-	-	-	-	-	-
	Given	175	74	40	-	1	1
SA Police	Made	-	-	-	-	-	-
	Refused	-	-	-	-	-	-
	Given	-	-	-	-	-	-
VIC Police	Made	1	1	-	-	-	-
	Refused	-	-	-	-	-	-
	Given	1	1	-	-	-	-
TOTAL	**Made**	**211**	**100**	**49**	**-**	**1**	**1**
	Refused	**-**	**-**	**-**	**-**	**-**	**-**
	Given	**211**	**100**	**49**	**-**	**1**	**1**

CHAPTER THREE – COMPUTER ACCESS WARRANTS

Applications for computer access warrants

Section 27A of the SD 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.

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

Section 27B of the SD 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 SD Act provides that this report must set out the number of remote applications made during the reporting period.

Section 27F of the SD 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 SD Act provides that the annual report must set out the number of applications for the extension of a computer access warrant that were made, and the number of extensions granted and refused (including reasons why applications were granted or refused) during the reporting period.

This information is presented in Table 7. In 2020–21, law enforcement agencies were issued 23 computer access warrants.

Table 7: Number of computer access warrants issued, remote applications made, and extensions granted– paragraphs 50(1)(a), 50(1)(d), 50(1)(e) and 50(1)(f)

Agency		Warrant Applications			Remote Applications			Extensions of Warrants		
		18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21
ACIC	Made	1	4	9	-	-	-	-	1	4
	Refused	-	-	-	-	-	-	-	-	-
	Issued	1	4	9	-	-	-	-	1	4
AFP	Made	8	18	13	-	-	-	2	10	23
	Refused	1	2	-	-	-	-	-	-	-
	Issued	7	16	13	-	-	-	2	10	23
LECC	Made	-	-	1	-	-	-	-	-	-
	Refused	-	-	-	-	-	-	-	-	-
	Issued	-	-	1	-	-	-	-	-	-
TOTAL	**Made**	**9**	**22**	**23**	**-**	**-**	**-**	**2**	**11**	**27**
	Refused	**1**	**2**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
	Issued	**8**	**20**	**23**	**-**	**-**	**-**	**2**	**11**	**27**

The ACIC advised it was granted extensions of computer access warrants to allow for the continuation of the operation/investigation; continued access to the target computer; more sufficient evidence to be gathered; and relevant offences, as defined in the SD Act, to be targeted.

The AFP advised it was granted extensions of computer access warrants due to ongoing investigations into serious and organised criminal activity.

International assistance applications for computer access warrants

Subsection 27A(4) of the SD 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 15CC 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.

Paragraphs 50(1)(aa) and 50(1)(ea) of the SD Act provide that this report must set out the number of international assistance applications made, and refused (including the reasons for any refusal) and the number of warrants issued as a result, 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 SD 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 2020–21, no law enforcement agencies applied for a computer access warrant as a result of an international assistance application. This remains the same as 2019-20.

Access to data in emergency circumstances

An appropriate authorising officer of a law enforcement agency may issue an emergency authorisation to authorise access data held in a computer. An emergency authorisation may only be issued in urgent circumstances when it is not practicable to apply for a warrant and:

- there is an imminent risk of serious violence to a person or substantial damage to property (section 28),
- a recovery order in relation to a child is in force (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).

Access to data under such an authorisation must be retrospectively approved by an eligible Judge or AAT member within 48 hours of the authorisation being issued.

Paragraphs 50(1)(b) and 50(1)(e) provide that this report must set out the number of applications for emergency authorisations made, refused (including the reasons for any refusal) and the number of authorisations given during the reporting period.

In 2020–21, no law enforcement agency made an emergency authorisation application for access to data held in a computer warrant. This remains the same as 2019-20.

CHAPTER FOUR – EFFECTIVENESS OF THE SD 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 can provide an indication of the effectiveness of the use of surveillance powers in the SD Act as a law enforcement investigative tool (although see further the interpretative note under Table 8 with respect to the limitations of this data).

This information is presented in Table 8. In 2020–21, information obtained under the SD Act contributed to 371 arrests, 50 prosecutions, and 42 convictions.

Table 8: 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		
	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21	18/19	19/20	20/21
ACIC	46	-	-	-	-	-	5	5	-	5	5	-
ACLEI	1	-	-	-	-	-	4	-	-	1	-	-
AFP	123	129	360	-	-	-	122	112	50	57	49	42
NSW Police	2	-	-	-	-	-	-	-	-	1	-	-
SA Police	-	1	-	-	-	-	-	-	-	-	-	-
VIC Police	3	1	-	-	-	-	1	-	-	-	-	-
WA Police	-	-	11	-	-	-	-	-	-	-	-	-
TOTAL	**175**	**131**	**371**	**-**	**-**	**-**	**132**	**117**	**50**	**64**	**54**	**42**

Interpretive note

The information presented in Table 8 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 SD Act as, in some cases, prosecutions may be initiated and convictions recorded without the need to give information obtained under the SD Act in evidence. In particular, agencies report that the use of the SD 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 SD 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

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

APPENDIX A – LIST OF TABLES

APPENDIX B – ABBREVIATIONS

Abbreviation	Name
AAT	Administrative Appeals Tribunal
ACIC	Australian Criminal Intelligence Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
LECC	Law Enforcement Conduct Commission
NSW Police	New South Wales Police
SA Police	South Australia Police
SD Act	*Surveillance Devices Act 2004*
VIC Police	Victoria Police
WA Police	Western Australia Police

NOTES

NOTES

NOTES

www.homeaffairs.gov.au