Australian Capital Territory

Crimes (Surveillance Devices) Act 2010

A2010-23

Republication No 8

Effective: 17 December 2021 – 10 February 2022

Republication date: 17 December 2021

Last amendment made by A2021-33

About this republication

The republished law

This is a republication of the *Crimes (Surveillance Devices) Act 2010* (including any amendment made under the *Legislation Act 2001*, part 11.3 (Editorial changes)) as in force on 17 December 2021. It also includes any commencement, amendment, repeal or expiry affecting this republished law to 17 December 2021.

The legislation history and amendment history of the republished law are set out in endnotes 3 and 4.

Kinds of republications

The Parliamentary Counsel's Office prepares 2 kinds of republications of ACT laws (see the ACT legislation register at www.legislation.act.gov.au):

- authorised republications to which the *Legislation Act 2001* applies
- unauthorised republications.

The status of this republication appears on the bottom of each page.

Editorial changes

The *Legislation Act 2001*, part 11.3 authorises the Parliamentary Counsel to make editorial amendments and other changes of a formal nature when preparing a law for republication. Editorial changes do not change the effect of the law, but have effect as if they had been made by an Act commencing on the republication date (see *Legislation Act 2001*, s 115 and s 117). The changes are made if the Parliamentary Counsel considers they are desirable to bring the law into line, or more closely into line, with current legislative drafting practice.

This republication does not include amendments made under part 11.3 (see endnote 1).

Uncommenced provisions and amendments

If a provision of the republished law has not commenced, the symbol **U** appears immediately before the provision heading. Any uncommenced amendments that affect this republished law are accessible on the ACT legislation register (www.legislation.act.gov.au). For more information, see the home page for this law on the register.

Modifications

If a provision of the republished law is affected by a current modification, the symbol **M** appears immediately before the provision heading. The text of the modifying provision appears in the endnotes. For the legal status of modifications, see the *Legislation Act 2001*, section 95.

Penalties

At the republication date, the value of a penalty unit for an offence against this law is $160 for an individual and $810 for a corporation (see *Legislation Act 2001*, s 133).

Australian Capital Territory

Crimes (Surveillance Devices) Act 2010

Contents

Page

Part 1 Preliminary

1 Name of Act 2
3 Dictionary 2
4 Notes 2
5 Offences against Act—application of Criminal Code etc 2
6 Purposes of Act 3
7 Relationship to other laws and matters 3
8 Investigation taken to be conducted in ACT 4

Part 2 Warrants

Division 2.1 Introduction

9 Kinds of warrant 5
10 Who may issue warrants? 5

Page

Division 2.2 Surveillance device warrants

11 Surveillance device warrant—application 6
12 Surveillance device warrant—remote application 7
13 Surveillance device warrant—deciding the application 8
14 What must a surveillance device warrant contain? 9
15 What a surveillance device warrant authorises 10
16 Extension and amendment of surveillance device warrant 13
17 Revocation of surveillance device warrant 14
18 Discontinuance of use of surveillance device under warrant 14

Division 2.3 Retrieval warrants

19 Retrieval warrant—application 15
20 Retrieval warrant—remote application 16
21 Retrieval warrant—deciding the application 16
22 What must a retrieval warrant contain? 17
23 What a retrieval warrant authorises 18
24 Revocation of retrieval warrant 19

Part 3 Emergency authorisations

24A Application of pt 3—integrity commission 21
25 Emergency authorisation—risk of serious personal violence or substantial property damage 21
26 Emergency authorisation—continued use of authorised surveillance device in participating jurisdiction 22
27 Application for approval after use of surveillance device under emergency authorisation 23
28 Consideration of application 24
29 Judge may approve emergency use of powers 25
30 Admissibility of evidence 26

Part 4 Recognition of corresponding warrants and authorisations

31 Corresponding warrants 27
32 Corresponding emergency authorisations 27

Page

Part 5 Compliance and monitoring

Division 5.1 Restrictions on use, communication and publication of information

33 What is *protected information*?—div 5.1 28
34 Prohibition on communication or publication of protected information 28
35 Dealing with records obtained by use of surveillance devices 33
36 Protection of surveillance device technologies and methods 33
37 Protected information in the custody of a court 34

Division 5.2 Reporting and record-keeping

38 Annual reports 35
39 Keeping documents connected with warrants and emergency authorisations 36
40 Other records to be kept 37
41 Register of warrants and emergency authorisations 39

Division 5.3 Inspections

42 Inspection of records by ombudsman 40

Division 5.4 General

43 Evidentiary certificates 41

Part 6 Miscellaneous

44 Delegation 43
45 Regulation-making power 43

Dictionary 44

Endnotes

1 About the endnotes 51
2 Abbreviation key 51
3 Legislation history 52
4 Amendment history 54
5 Earlier republications 56

Australian Capital Territory

Crimes (Surveillance Devices) Act 2010

An Act to provide for the authorisation of the installation, use, maintenance and retrieval of surveillance devices for law enforcement purposes

Part 1 Preliminary

1 Name of Act

This Act is the *Crimes (Surveillance Devices) Act 2010*.

3 Dictionary

The dictionary at the end of this Act is part of this Act.

Note 1 The dictionary at the end of this Act defines certain terms used in this Act, and includes references (signpost definitions) to other terms defined elsewhere in this Act.

For example, the signpost definition '***protected information***, for division 5.1—see section 33.' means that the term 'protected information' is defined in that section for that division.

Note 2 A definition in the dictionary (including a signpost definition) applies to the entire Act unless the definition, or another provision of the Act, provides otherwise or the contrary intention otherwise appears (see Legislation Act, s 155 and s 156 (1)).

4 Notes

A note included in this Act is explanatory and is not part of this Act.

Note See the Legislation Act, s 127 (1), (4) and (5) for the legal status of notes.

5 Offences against Act—application of Criminal Code etc

Other legislation applies in relation to offences against this Act.

Note 1 *Criminal Code*

The Criminal Code, ch 2 applies to all offences against this Act (see Code, pt 2.1).

The chapter sets out the general principles of criminal responsibility (including burdens of proof and general defences), and defines terms used for offences to which the Code applies (eg ***conduct***, ***intention***, ***recklessness*** and ***strict liability***).

Note 2 *Penalty units*

The Legislation Act, s 133 deals with the meaning of offence penalties that are expressed in penalty units.

6 Purposes of Act

The main purposes of this Act are—

(a) to establish procedures for law enforcement officers to obtain warrants or emergency authorisations for the installation, use, maintenance and retrieval of surveillance devices in criminal and corrupt conduct investigations, including investigations extending beyond the ACT; and

(b) to recognise warrants and emergency authorisations issued in other jurisdictions; and

(c) to restrict the use, communication and publication of information obtained through the use of surveillance devices or otherwise connected with surveillance device operations; and

(d) to impose requirements for the secure storage and destruction of records, and the making of reports to the Legislative Assembly, in connection with surveillance device operations.

7 Relationship to other laws and matters

(1) This Act does not affect any other territory law that prohibits or regulates the use of surveillance devices wholly within the ACT.

Note ***Territory law*** includes the common law (see Legislation Act, dict, pt 1, def ***territory law*** and ***law***, of the Territory).

(2) A function conferred in relation to the activities of the Australian Crime Commission under this Act is only conferred for the purpose of the function conferred on the Australian Crime Commission under the *Australian Crime Commission (ACT) Act 2003* relating to suspected serious and organised crime as defined in that Act.

(3) This Act does not stop a law enforcement officer from using an optical surveillance device in a place where the presence of a police officer is not an offence.

(4) This Act does not limit a discretion that a court has—

(a) to admit or exclude evidence in any proceeding; or

(b) to stay criminal proceedings in the interests of justice.

(5) To remove any doubt, a warrant may be issued, or an emergency authorisation given, in the ACT under this Act for the installation, use, maintenance or retrieval of a surveillance device in the ACT or a participating jurisdiction or both.

(6) The following Acts do not apply in relation to activities, documents and records under this Act:

(a) the *Freedom of Information Act 2016*;

(b) the *Territory Records Act 2002*.

8 Investigation taken to be conducted in ACT

For this Act, an investigation into a relevant offence or corrupt conduct is taken to be conducted in the ACT, whether or not it is also conducted in another jurisdiction, if a law enforcement officer participates in the investigation.

Note This section is intended to cover the situation where a law enforcement officer of the ACT is conducting or participating in an investigation wholly in another jurisdiction for the purposes of an offence or corrupt conduct against a territory law (eg a law enforcement of the ACT officer is investigating a conspiracy to import drugs into the ACT from NSW and all the evidence of the offence is in NSW).

Part 2 Warrants

Division 2.1 Introduction

9 Kinds of warrant

(1) The following kinds of warrant may be issued under this part:

(a) a surveillance device warrant;

(b) a retrieval warrant.

(2) A warrant may be issued in relation to 1 or more kinds of surveillance device.

10 Who may issue warrants?

(1) A judge may issue any warrant under this part.

Note ***Judge*** includes the associate judge (see dict).

(2) A magistrate may issue—

(a) a surveillance device warrant that authorises the use of a tracking device only; or

(b) a retrieval warrant in relation to a tracking device authorised under a warrant mentioned in paragraph (a), if a magistrate issued the original warrant.

Division 2.2 Surveillance device warrants

11 Surveillance device warrant—application

(1) A law enforcement officer (or another person on the officer's behalf) may apply for the issue of a surveillance device warrant if the law enforcement officer suspects or believes on reasonable grounds that—

(a) either—

(i) a relevant offence has been, is being, is about to be, or is likely to be committed; or

(ii) corrupt conduct has been, is being, is about to be, or is likely to be engaged in; and

(b) an investigation into that offence or conduct is being, will be or is likely to be conducted in the ACT, in the ACT and in 1 or more participating jurisdictions or in 1 or more participating jurisdictions; and

(c) the use of a surveillance device in the ACT, in the ACT and in 1 or more participating jurisdictions or in 1 or more participating jurisdictions is or will be necessary in the course of that investigation for the purpose of enabling evidence or information to be obtained of the commission of the relevant offence or corrupt conduct or the identity or location of the offender.

(2) The application may be made to—

(a) a judge; or

(b) for an application for a surveillance device warrant authorising the use of a tracking device only—a magistrate.

(3) An application—

(a) must state—

(i) the name of the applicant; and

(ii) the nature and duration of the warrant sought, including the kind of surveillance device sought to be authorised; and

(b) subject to this section, must be supported by an affidavit setting out the grounds on which the warrant is sought.

(4) An application for a warrant may be made before an affidavit is prepared or sworn if a law enforcement officer believes that—

(a) the immediate use of a surveillance device is necessary for a purpose mentioned in subsection (1) (c); and

(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made.

(5) If subsection (4) applies, the applicant must—

(a) give as much information as the judge or magistrate considers is reasonably practicable in the circumstances; and

(b) not later than 72 hours after making the application, send a sworn affidavit to the judge or magistrate, whether or not a warrant has been issued.

(6) An application for a warrant must not be heard in open court.

12 Surveillance device warrant—remote application

(1) If a law enforcement officer believes that it is impracticable for an application for a surveillance device warrant to be made in person, the application may be made under section 11 by telephone, fax, email or any other means of communication.

(2) If transmission by fax is available and an affidavit has been prepared, the person applying must send a copy of the affidavit, whether sworn or unsworn, to the judge or magistrate who is to decide the application.

13 Surveillance device warrant—deciding the application

(1) A judge or magistrate may issue a surveillance device warrant if satisfied that—

(a) there are reasonable grounds for the suspicion or belief founding the application for the warrant; and

(b) for an unsworn application—it would have been impracticable for an affidavit to have been prepared or sworn before the application was made; and

(c) for a remote application—it would have been impracticable for the application to have been made in person.

(2) In deciding whether a surveillance device warrant should be issued, the judge or magistrate must have regard to the following:

(a) the nature and gravity of the alleged offence or corrupt conduct in relation to which the warrant is sought;

(b) the extent to which the privacy of any person is likely to be affected;

(c) the existence of any alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation;

(d) the evidentiary or intelligence value of any information sought to be obtained;

(e) any previous warrant sought or issued under this division or a corresponding law (if known) in connection with the same offence or corrupt conduct.

14 What must a surveillance device warrant contain?

(1) A surveillance device warrant must—

(a) state that the judge or magistrate is satisfied of the matters mentioned in section 13 (1) and has had regard to the matters mentioned in section 13 (2); and

(b) state the following:

(i) the name of the applicant;

(ii) the alleged offence or corrupt conduct in relation to which the warrant is issued;

(iii) the date the warrant is issued;

(iv) the kind of surveillance device authorised to be used;

(v) if the warrant authorises the use of a surveillance device on premises—the premises where the use of the surveillance device is authorised;

(vi) if the warrant authorises the use of a surveillance device in or on an object or class of object—the object or class of object in or on which the use of the surveillance device is authorised;

(vii) if the warrant authorises the use of a surveillance device in relation to the conversations, activities or geographical location of a person—the name of the person (if known);

(viii) the period (not more than 90 days) during which the warrant is in force;

(ix) the name of the law enforcement officer primarily responsible for executing the warrant;

(x) any conditions subject to which premises may be entered, or a surveillance device may be used, under the warrant.

(2) For a warrant mentioned in subsection (1) (b) (vii), if the identity of the person is unknown, the warrant must state that fact.

(3) A warrant must be signed by the person issuing it and include the person's name.

(4) If the judge or magistrate issues a warrant on a remote application, the judge or magistrate must—

(a) tell the applicant—

(i) the terms of the warrant; and

(ii) the date and time the warrant was issued; and

(b) enter the terms and date mentioned in paragraph (a) in a register kept by the judge or magistrate for the purpose; and

(c) give the applicant a copy of the warrant as soon as practicable.

15 What a surveillance device warrant authorises

(1) A surveillance device warrant may authorise, as stated in the warrant, 1 or more of the following:

(a) the use of a surveillance device on stated premises;

(b) the use of a surveillance device in or on a stated object or class of objects;

(c) the use of a surveillance device in relation to the conversations, activities or geographical location of a stated person or a person whose identity is unknown.

(2) A surveillance device warrant authorises—

(a) for a warrant mentioned in subsection (1) (a)—

(i) the installation, use and maintenance of a surveillance device of the kind stated in the warrant on the stated premises; and

(ii) the entry, by force if necessary, onto the premises, or other stated premises adjoining or providing access to the premises, for a purpose mentioned in subparagraph (i) or subsection (3);

(b) for a warrant mentioned in subsection (1) (b)—

(i) the installation, use and maintenance of a surveillance device of the kind stated in the warrant in or on the stated object or an object of the stated class; and

(ii) the entry, by force if necessary, onto any premises where the object, or an object of the class, is believed on reasonable grounds to be or is likely to be, or other premises adjoining or providing access to those premises, for a purpose mentioned in subparagraph (i) or subsection (3);

(c) for a warrant mentioned in subsection (1) (c)—

(i) the installation, use and maintenance of a surveillance device of the kind stated in the warrant, on premises where the person is believed on reasonable grounds to be or likely to be; and

(ii) the entry, by force if necessary, onto the premises mentioned in subparagraph (i), or other premises adjoining or providing access to those premises, for a purpose mentioned in subparagraph (i) or subsection (3).

(3) Each surveillance device warrant also authorises the following:

(a) the retrieval of the surveillance device;

(b) the installation, use, maintenance and retrieval of any enhancement equipment in relation to the surveillance device;

(c) the temporary removal of an object or vehicle from premises for the purpose of the installation, maintenance or retrieval of the surveillance device or enhancement equipment and the return of the object or vehicle to the premises;

(d) the breaking open of anything for the purpose of the installation, maintenance or retrieval of the surveillance device or enhancement equipment;

(e) the connection of the surveillance device or enhancement equipment to an electricity supply system and the use of electricity from that system to operate the surveillance device or enhancement equipment;

(f) the connection of the surveillance device or enhancement equipment to any object or system that may be used to transmit information in any form and the use of that object or system in connection with the operation of the surveillance device or enhancement equipment;

(g) the provision of assistance or technical expertise to the law enforcement officer primarily responsible for executing the warrant in the installation, use, maintenance or retrieval of the surveillance device or enhancement equipment.

(4) A surveillance device warrant may authorise the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to the installation, use, maintenance or retrieval of a surveillance device or enhancement equipment under the warrant.

(5) A law enforcement officer may use a surveillance device under a warrant only if the officer is acting in the performance of the officer's duty.

(6) This section applies to a surveillance device warrant subject to any conditions stated in the warrant.

(7) Nothing in this section authorises the doing of anything for which a warrant would be required under the *Telecommunications (Interception and Access) Act 1979* (Cwlth).

16 Extension and amendment of surveillance device warrant

(1) A law enforcement officer to whom a surveillance device warrant has been issued (or another person on the officer's behalf) may apply, at any time before the expiry of the warrant—

(a) for an extension of the warrant for a period not exceeding 90 days after the day when it would otherwise expire; or

(b) for an amendment of any of the other terms of the warrant.

(2) The application must be made to—

(a) a judge, if the warrant was issued by a judge; or

(b) a magistrate, if the warrant was issued by a magistrate.

(3) Section 11 (Surveillance device warrant—application) and section 12 (Surveillance device warrant—remote application) apply, with any necessary changes, to an application under this section as if it were an application for the warrant.

(4) The judge or magistrate may grant an application, subject to any conditions the judge or magistrate thinks fit, if satisfied that the matters mentioned in section 13 (1) (Surveillance device warrant—deciding the application) still exist, having regard to the matters in section 13 (2).

(5) If the judge or magistrate grants the application, the judge or magistrate must endorse the new expiry date or the other amended term on the original warrant.

(6) An application may be made under this section more than once.

17 Revocation of surveillance device warrant

(1) A surveillance device warrant may be revoked at any time before the end of the period of validity stated in it by—

(a) a judge, if a judge issued the warrant; or

(b) a magistrate, if a magistrate issued the warrant.

(2) A judge or magistrate may revoke a surveillance device warrant on application by or on behalf of a law enforcement officer.

(3) A judge or magistrate who revokes a warrant must give notice of the revocation to the chief officer of the law enforcement agency of which the law enforcement officer to whom the warrant was issued is a member.

(4) If the judge or magistrate revokes the warrant on the application of a law enforcement officer, the judge or magistrate is taken to have notified the chief officer under subsection (3) when the judge or magistrate revokes the warrant.

18 Discontinuance of use of surveillance device under warrant

(1) This section applies if a surveillance device warrant is issued to a law enforcement officer of a law enforcement agency.

(2) If the chief officer of the law enforcement agency is satisfied that the use of a surveillance device under the warrant is no longer necessary for the purpose of enabling evidence to be obtained of the commission of the relevant offence or corrupt conduct or the identity or location of the offender, the chief officer must—

(a) take the steps necessary to ensure that use of the surveillance device authorised by the warrant is discontinued as soon as practicable; and

(b) ensure an application is made for the revocation of the warrant under section 17.

(3) If the chief officer is notified that the warrant has been revoked under section 17, the chief officer must take the steps necessary to ensure that use of the surveillance device authorised by the warrant is discontinued immediately.

(4) If the law enforcement officer to whom the warrant is issued, or who is primarily responsible for executing the warrant, believes that use of a surveillance device under the warrant is no longer necessary for the purpose of enabling evidence to be obtained of the commission of the relevant offence or corrupt conduct or the identity or location of the offender, the officer must tell the chief officer of the law enforcement agency immediately.

Division 2.3 Retrieval warrants

19 Retrieval warrant—application

(1) A law enforcement officer (or another person on the officer's behalf) may apply for the issue of a retrieval warrant in relation to a surveillance device that—

(a) was lawfully installed on premises, or in or on an object, under a surveillance device warrant; and

(b) the law enforcement officer suspects or believes on reasonable grounds is still on those premises or in or on that object, or on other premises or in or on another object.

(2) The application may be made to—

(a) a judge; or

(b) for an application for a retrieval warrant authorising the retrieval of a tracking device only—a magistrate.

(3) Subject to this section, an application must be supported by an affidavit setting out the grounds on which the warrant is sought.

(4) An application for a retrieval warrant may be made before an affidavit is prepared or sworn if a law enforcement officer believes that—

(a) the immediate retrieval of a surveillance device is necessary; and

(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made.

(5) If subsection (4) applies, the applicant must—

(a) give as much information as the judge or magistrate considers is reasonably practicable in the circumstances; and

(b) not later than 72 hours after making the application, send a sworn affidavit to the judge or magistrate who determined the application, whether or not a warrant has been issued.

(6) An application for a warrant must not be heard in open court.

20 Retrieval warrant—remote application

(1) If a law enforcement officer believes that it is impracticable for an application for a retrieval warrant to be made in person, the application may be made under section 19 by telephone, fax, email or any other means of communication.

(2) If transmission by fax is available and an affidavit has been prepared, the person applying must send a copy of the affidavit, whether sworn or unsworn, to the judge or magistrate who is to decide the application.

21 Retrieval warrant—deciding the application

(1) A judge or magistrate may issue a retrieval warrant if satisfied that—

(a) there are reasonable grounds for the suspicion or belief founding the application for the warrant; and

(b) for an unsworn application—it would have been impracticable for an affidavit to have been prepared or sworn before the application was made; and

(c) for a remote application—it would have been impracticable for the application to have been made in person.

(2) In deciding whether a retrieval warrant should be issued, the judge or magistrate must have regard to—

(a) the extent to which the privacy of any person is likely to be affected; and

(b) the public interest in retrieving the device sought to be retrieved.

22 What must a retrieval warrant contain?

(1) A retrieval warrant must—

(a) state that the judge or magistrate is satisfied of the matters mentioned in section 21 (1) and has had regard to the matters mentioned in section 21 (2); and

(b) state the following:

(i) the name of the applicant;

(ii) the date the warrant is issued;

(iii) the kind of surveillance device authorised to be retrieved;

(iv) the premises or object from which the surveillance device is to be retrieved;

(v) the period (not more than 90 days) during which the warrant is in force;

(vi) the name of the law enforcement officer primarily responsible for executing the warrant;

(vii) any conditions subject to which premises may be entered under the warrant.

(2) A warrant must be signed by the person issuing it and include the person's name.

(3) If the judge or magistrate issues a warrant on a remote application, the judge or magistrate must—

(a) tell the applicant—

(i) the terms of the warrant; and

(ii) the date and time the warrant was issued; and

(b) enter the terms and date mentioned in paragraph (a) in a register kept by the judge or magistrate for the purpose; and

(c) give the applicant a copy of the warrant as soon as practicable.

(4) Unless sooner executed or revoked, a retrieval warrant remains in force for the period stated in the warrant.

23 What a retrieval warrant authorises

(1) A retrieval warrant authorises the following:

(a) the retrieval of the surveillance device stated in the warrant and any enhancement equipment in relation to the device;

(b) the entry, by force if necessary, onto the premises where the surveillance device is believed on reasonable grounds to be, or other premises adjoining or providing access to those premises, for the purpose of retrieving the device and equipment;

(c) the breaking open of any thing for the purpose of retrieving the device and equipment;

(d) if the device or equipment is installed on or in an object, the temporary removal of the object from any premises where it is located for the purpose of retrieving the device and equipment and the return of the object to those premises;

(e) the provision of assistance or technical expertise to the law enforcement officer primarily responsible for executing the warrant in the retrieval of the device or equipment.

(2) If the retrieval warrant authorises the retrieval of a tracking device, the warrant also authorises the use of the tracking device and any enhancement equipment in relation to the device solely for the purposes of the location and retrieval of the device or equipment.

(3) A retrieval warrant may authorise the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to the retrieval of a surveillance device or enhancement equipment under the warrant.

(4) This section applies to a retrieval warrant subject to any conditions stated in the warrant.

24 Revocation of retrieval warrant

(1) A retrieval warrant may be revoked at any time before the end of the period of validity stated in it by—

(a) a judge, if a judge issued the warrant; or

(b) a magistrate, if a magistrate issued the warrant.

(2) A judge or magistrate may revoke a retrieval warrant on application by or on behalf of a law enforcement officer.

(3) A judge or magistrate who revokes a warrant must give notice of the revocation to the chief officer of the law enforcement agency of which the law enforcement officer to whom the warrant was issued is a member.

(4) If the judge or magistrate revokes the warrant on the application of a law enforcement officer, the judge or magistrate is taken to have notified the chief officer under subsection (3) when the judge or magistrate revokes the warrant.

(5) If the chief officer of a law enforcement agency is satisfied that the grounds for issue of a retrieval warrant to a law enforcement officer of the agency no longer exist, the chief officer must ensure an application is made for the revocation of the warrant under this section.

(6) If the law enforcement officer to whom a retrieval warrant has been issued, or who is primarily responsible for executing a retrieval warrant, believes that the grounds for issue of the warrant no longer exist, the officer must tell the chief officer of the law enforcement agency immediately.

Part 3 Emergency authorisations

24A Application of pt 3—integrity commission

This part does not apply to a law enforcement agency that is the integrity commission.

25 Emergency authorisation—risk of serious personal violence or substantial property damage

(1) A law enforcement officer of a law enforcement agency may apply to the chief officer of the agency for an emergency authorisation for the use of a surveillance device if, in the course of an investigation, the law enforcement officer suspects or believes on reasonable grounds that—

(a) an imminent threat of serious violence to a person or substantial damage to property exists; and

(b) the use of a surveillance device is immediately necessary for the purpose of dealing with that threat; and

(c) the circumstances are so serious and the matter is of such urgency that the use of a surveillance device is warranted; and

(d) it is not practicable in the circumstances to apply for a surveillance device warrant.

Example—par (d)

the law enforcement officer has tried, unsuccessfully, to contact an on-call duty magistrate or judge by telephone

(2) An application may be made orally, in writing or by telephone, fax, email or any other means of communication.

(3) The chief officer may give an emergency authorisation for the use of a surveillance device on an application under subsection (1) if satisfied that there are reasonable grounds for the suspicion or belief founding the application.

(4) An emergency authorisation given under this section may authorise the law enforcement officer to whom it is given to do anything that a surveillance device warrant may authorise the officer to do.

26 Emergency authorisation—continued use of authorised surveillance device in participating jurisdiction

(1) A law enforcement officer of a law enforcement agency may apply to the chief officer of the agency for an emergency authorisation for the use of a surveillance device if—

(a) use of the surveillance device in the ACT is authorised under a territory law, in connection with an investigation into a relevant offence; and

(b) the law enforcement officer suspects or believes on reasonable grounds that—

(i) the investigation in relation to which the surveillance device is authorised in the ACT is likely to extend to a participating jurisdiction; and

(ii) the use of the surveillance device in a participating jurisdiction is immediately necessary to prevent the loss of any evidence; and

(iii) the circumstances are so serious and the matter is of such urgency that the use of the surveillance device in the participating jurisdiction is warranted; and

(iv) it is not practicable in the circumstances to apply for a surveillance device warrant.

Example—par (b) (iv)

the law enforcement officer has tried, unsuccessfully, to contact an on-call duty magistrate or judge by telephone

(2) An application may be made orally, in writing or by telephone, fax, email or any other means of communication.

(3) The chief officer may give an emergency authorisation for the use of a surveillance device on an application under subsection (1) if satisfied that—

(a) use of the surveillance device in the ACT is authorised under a territory law, in connection with an investigation into a relevant offence; and

(b) there are reasonable grounds for the suspicion or belief founding the application.

(4) An emergency authorisation given under this section may authorise the law enforcement officer to whom it is given to do anything that a surveillance device warrant may authorise the officer to do.

27 Application for approval after use of surveillance device under emergency authorisation

(1) Within 2 working days after giving an emergency authorisation, the chief officer (or another person on the officer's behalf) must apply to a judge for approval of the exercise of powers under the emergency authorisation.

(2) An application—

(a) must state—

(i) the name of the applicant; and

(ii) the kind of surveillance device sought to be approved and, if a warrant is sought, the nature and duration of the warrant; and

(b) must be supported by an affidavit setting out the grounds on which the approval (and warrant, if any) is sought.

(3) The judge may refuse to consider the application until the applicant gives the judge all the information the judge requires about the application in the way the judge requires.

(4) An application must not be heard in open court.

28 Consideration of application

(1) Before deciding an application for approval in relation to an emergency authorisation given under section 25 (Emergency authorisation—risk of serious personal violence or substantial property damage), the judge must, in particular, and being mindful of the intrusive nature of using a surveillance device, consider the following:

(a) the nature of the risk of serious violence to a person or substantial damage to property;

(b) the extent to which issuing a surveillance device warrant would have helped reduce or avoid the risk;

(c) the extent to which law enforcement officers could have used alternative methods of investigation to help reduce or avoid the risk;

(d) how much the use of alternative methods of investigation could have helped reduce or avoid the risk;

(e) how much the use of alternative methods of investigation would have prejudiced the safety of the person or property because of delay or for another reason;

(f) whether or not it was practicable in the circumstances to apply for a surveillance device warrant.

(2) Before deciding an application for approval in relation to an emergency authorisation given under section 26 (Emergency authorisation—continued use of authorised surveillance device in participating jurisdiction), the judge must, in particular, and being mindful of the intrusive nature of using a surveillance device, consider the following:

(a) the nature of the risk of the loss of evidence;

(b) the extent to which issuing a surveillance device warrant would have helped reduce or avoid the risk;

(c) the terms of the existing authorisation for the use of the surveillance device;

(d) whether or not it was practicable in the circumstances to apply for a surveillance device warrant.

29 Judge may approve emergency use of powers

(1) After considering an application for approval in relation to an emergency authorisation given under section 25 (Emergency authorisation—risk of serious personal violence or substantial property damage), the judge may approve the application if satisfied that there were reasonable grounds to suspect or believe that—

(a) there was a risk of serious violence to a person or substantial damage to property; and

(b) using a surveillance device may have helped reduce the risk; and

(c) it was not practicable in the circumstances to apply for a surveillance device warrant.

(2) After considering an application for approval in relation to an emergency authorisation given under section 26 (Emergency authorisation—continued use of authorised surveillance device in participating jurisdiction), the judge may approve the application if satisfied that—

(a) use of the surveillance device in the ACT was authorised under a territory law, in connection with an investigation into a relevant offence; and

(b) there were reasonable grounds to suspect or believe that—

(i) there was a risk of loss of evidence; and

(ii) using the surveillance device in a participating jurisdiction may have helped reduce the risk; and

(c) it was not practicable in the circumstances to apply for a surveillance device warrant.

(3) If the judge approves an application under this section, the judge may issue a surveillance device warrant for the continued use of the surveillance device as if the application were an application for a surveillance device warrant under division 2 (Surveillance device warrants).

(4) If the judge does not approve an application under this section, the judge may order that the use of the surveillance device cease.

(5) The judge may order that any information obtained from or relating to the exercise of powers under the emergency authorisation or any record of that information be dealt with in the way stated in the order.

30 Admissibility of evidence

If the exercise of powers under an emergency authorisation is approved under section 29, evidence obtained because of the exercise of those powers is not inadmissible in any proceeding only because the evidence was obtained before the approval.

Part 4 Recognition of corresponding warrants and authorisations

31 Corresponding warrants

A corresponding warrant may be executed in the ACT in accordance with its terms as if it were a surveillance device warrant or retrieval warrant issued under part 2 (Warrants).

32 Corresponding emergency authorisations

(1) A corresponding emergency authorisation authorises the use of a surveillance device in accordance with its terms in the ACT, as if it were an emergency authorisation given under part 3 (Emergency authorisations).

(2) Subsection (1) does not apply at any time after a judge orders, under a provision of a corresponding law that corresponds to section 29 (4) (Judge may approve emergency use of powers), that the use of a surveillance device under the corresponding emergency authorisation cease.

Part 5 Compliance and monitoring

Division 5.1 Restrictions on use, communication and publication of information

33 What is *protected information*?—div 5.1

In this division:

protected information means—

(a) any information obtained from the use of a surveillance device under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or

(b) any information relating to—

(i) an application for, issue of, existence of or expiry of a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or

(ii) an application for approval of powers exercised under an emergency authorisation; or

(iii) an application under a corresponding law for approval of powers exercised under a corresponding emergency authorisation.

34 Prohibition on communication or publication of protected information

(1) A person commits an offence if—

(a) the person uses information; and

(b) the information is protected information; and

(c) the use of the information is not permitted by this section; and

(d) the person is reckless about whether the use of the information is not permitted by this section.

Maximum penalty: imprisonment for 2 years.

Note The fault element of recklessness can be satisfied by proof of intention, knowledge or recklessness (see Criminal Code, s 20 (4)).

(2) A person commits an offence if—

(a) the person communicates information; and

(b) the information is protected information; and

(c) the communication of the information is not permitted by this section; and

(d) the person is reckless about whether the communication of the information is not permitted by this section.

Maximum penalty: imprisonment for 2 years.

(3) A person commits an offence if—

(a) the person publishes information; and

(b) the information is protected information; and

(c) the publication of the information is not permitted by this section; and

(d) the person is reckless about whether the publication of the information is not permitted by this section.

Maximum penalty: imprisonment for 2 years.

(4) A person commits an offence if the person commits an offence against subsection (1), (2) or (3) in circumstances in which the person—

(a) intends to endanger the health or safety of anyone; or

(b) is reckless about whether the disclosure of the information endangers or will endanger the health or safety of anyone.

Maximum penalty: imprisonment for 10 years.

(5) A person commits an offence if the person commits an offence against subsection (1), (2) or (3) in circumstances in which the person—

(a) intends to prejudice the effective conduct of an investigation; or

(b) is reckless about whether the disclosure of the information prejudices or will prejudice the effective conduct of an investigation.

Maximum penalty: imprisonment for 10 years.

(6) Subsections (1) to (5) do not apply to—

(a) the use, communication or publication of—

(i) any information if the information has been disclosed in proceedings in open court; or

(ii) any information if the information has entered the public domain; or

(b) the use or communication of protected information by a person if the person believes on reasonable grounds that the use or communication is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property; or

(c) the communication to the Director-General (within the meaning of the *Australian Security Intelligence Organisation Act 1979* (Cwlth)) of protected information if the protected information relates or appears to relate to activities prejudicial to security (within the meaning of that Act); or

(d) the use or communication of information mentioned in paragraph (c) by an officer of the Australian Security Intelligence Organisation if the use or communication is in the performance of the officer's official functions; or

(e) the use or communication of information to a foreign country or an appropriate authority of a foreign country if the use or communication is in accordance with the *Mutual Assistance in Criminal Matters Act 1987* (Cwlth).

(7) Protected information may be used, communicated or published if it is necessary to do so for any of the following purposes:

(a) the investigation of a relevant offence within the meaning of this Act or a relevant offence within the meaning of a corresponding law;

(b) the investigation of corrupt conduct under the *Integrity Commission Act 2018*;

(c) the making of a decision whether or not to bring a prosecution for a relevant offence within the meaning of this Act or a relevant offence within the meaning of a corresponding law;

(d) a relevant proceeding within the meaning of this Act or a relevant proceeding within the meaning of a corresponding law;

(e) an investigation of a complaint against, or the conduct of, a public officer within the meaning of this Act or a public officer within the meaning of a corresponding law;

(f) the making of a decision in relation to the appointment, re-appointment, term of appointment, termination or retirement of a person mentioned in paragraph (e);

(g) the keeping of records and the making of reports by—

(i) a law enforcement agency in accordance with the obligations imposed by division 5.2 (Reporting and record-keeping); or

(ii) a law enforcement agency (within the meaning of a corresponding law) in accordance with the obligations imposed by provisions of the corresponding law that correspond to division 5.2;

(h) an inspection by the ombudsman under section 42 (Inspection of records by ombudsman) or an inspection under a provision of a corresponding law that corresponds to section 42;

(i) an investigation under the *Information Privacy Act 2014* or another law of the Territory, a participating jurisdiction or the Commonwealth concerning the privacy of personal information.

(8) Subsections (6) (c) and (d) and (7) (a), (c) and (d) do not authorise the use, communication or publication of protected information in relation to an emergency authorisation or corresponding emergency authorisation unless the use of powers under that emergency authorisation has been approved under section 29 (Judge may approve emergency use of powers) or the provisions of a corresponding law that correspond to section 29.

(9) A reference in subsection (8) to a relevant offence (whether of the ACT or another jurisdiction) is a reference to any relevant offence of the relevant jurisdiction, whether or not it is the offence of the relevant jurisdiction in relation to which the relevant warrant or emergency authorisation was issued or given.

35 Dealing with records obtained by use of surveillance devices

(1) The chief officer of a law enforcement agency must cause—

(a) every record or report obtained by use of a surveillance device by a law enforcement officer of the agency under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation to be kept in a secure place that is not accessible to people who are not entitled to deal with the record or report; and

(b) any record or report mentioned in paragraph (a) to be destroyed, if satisfied that it is not likely to be required in connection with a purpose mentioned in section 34 (6) or (7).

(2) Subsection (1) does not apply to a record or report that is received into evidence in legal proceedings or disciplinary proceedings.

36 Protection of surveillance device technologies and methods

(1) In any proceeding, a person may object to the disclosure of information on the ground that the information, if disclosed, could reasonably be expected to reveal details of surveillance device technology or methods of installation, use or retrieval of surveillance devices.

(2) If the person conducting or presiding over the proceeding is satisfied that the ground of objection is made out, the person may order that the person who has the information not be required to disclose it in the proceeding.

(3) In determining whether or not to make an order under subsection (2), the person conducting or presiding over the proceeding must take into account whether disclosure of the information—

(a) is necessary for the fair trial of the defendant; or

(b) is in the public interest.

(4) Subsection (2) does not affect a provision of another law under which a law enforcement officer cannot be compelled to disclose information or make statements in relation to the information.

(5) If the person conducting or presiding over a proceeding is satisfied that publication of any information disclosed in the proceeding could reasonably be expected to reveal details of surveillance device technology or methods of installation, use or retrieval of surveillance devices, the person must make any orders prohibiting or restricting publication of the information that the person considers necessary to ensure that those details are not revealed.

(6) Subsection (5) does not apply to the extent that the person conducting or presiding over the proceeding considers that the interests of justice require otherwise.

(7) In this section:

proceeding includes—

(a) a proceeding before a court, tribunal or Royal Commission; and

(b) an examination before the integrity commission.

37 Protected information in the custody of a court

A person is not entitled to search any protected information in the custody of a court unless the court otherwise orders in the interests of justice.

Division 5.2 Reporting and record-keeping

38 Annual reports

(1) The chief officer of a law enforcement agency must give a written report to the Minister that includes the following information in relation to each financial year:

(a) the number of applications for warrants by and the number of warrants issued to law enforcement officers of the agency during the year;

(b) the number of applications for emergency authorisations by and the number of emergency authorisations given to law enforcement officers of the agency during the year;

(c) the number of remote applications for warrants by law enforcement officers of the agency during the year;

(d) the number of applications for warrants or emergency authorisations by law enforcement officers of the agency that were refused during the year, and the reasons for refusal;

(e) the number of applications for extensions of warrants by law enforcement officers of the agency during the year, the number of extensions granted or refused and the reasons why the extensions were granted or refused;

(f) the number of arrests made by law enforcement officers of the agency during the year on the basis (wholly or partly) of information obtained by the use of a surveillance device under a warrant or emergency authorisation;

(g) the number of prosecutions that were commenced in the ACT during the year in which information obtained by the use of a surveillance device under a warrant or emergency authorisation was given in evidence and the number of those prosecutions in which a person was found guilty;

(h) any other information relating to the use of surveillance devices and the administration of this Act that the Minister considers appropriate.

(2) The information mentioned in subsection (1) (a) and (b) must be presented in a way that identifies the number of warrants issued and emergency authorisations given in relation to each different kind of surveillance device.

(3) The report must be given to the Minister as soon as practicable after the end of each financial year, and in any event within 3 months after the end of the financial year.

(4) The Minister must present a copy of the report to the Legislative Assembly within 15 sitting days after the day the Minister receives it.

39 Keeping documents connected with warrants and emergency authorisations

The chief officer of a law enforcement agency must cause the following to be kept:

(a) each warrant issued to a law enforcement officer of the agency;

(b) each notice given to the chief officer under section 17 (3) (Revocation of surveillance device warrant) of revocation of a warrant;

(c) each emergency authorisation given to a law enforcement officer of the agency;

(d) each application made by a law enforcement officer of the agency for an emergency authorisation;

(e) a copy of each application made by a law enforcement officer of the agency for the following:

(i) a warrant;

(ii) extension, amendment or revocation of a warrant;

(iii) approval of the exercise of powers under an emergency authorisation;

(f) a copy of each certificate issued by the chief officer, or person assisting the officer, under section 43 (Evidentiary certificates).

40 Other records to be kept

The chief officer of a law enforcement agency must keep the following records:

(a) a statement as to whether each application made by a law enforcement officer of the agency for a warrant, or extension, amendment or revocation of a warrant, was granted, refused or withdrawn;

(b) for each warrant issued to a law enforcement officer of the agency, a statement about whether the warrant was executed;

(c) for each surveillance device warrant mentioned in a statement under paragraph (b) that was executed, a statement setting out the following information:

(i) the name of each person involved in the execution of the warrant;

(ii) the kind of surveillance device used;

(iii) the period during which the device was used;

(iv) the name, if known, of any person whose conversations or activities were overheard, recorded, monitored, listened to or observed by the use of the device;

(v) the name, if known, of any person whose geographical location was worked out by the use of a tracking device;

(vi) details of any premises on which the device was installed or any place at which the device was used;

(vii) details of any object in or on which the device was installed or any premises where the object was located when the device was installed;

(viii) details of the benefit to the investigation of the use of the device and of the general use made or to be made of any evidence or information obtained by the use of the device;

(ix) details of the compliance with the conditions (if any) to which the warrant was subject;

(x) if the warrant was extended or amended, the number of extensions or amendments and the reasons for them;

(d) for each retrieval warrant mentioned in a statement under paragraph (b) that was executed, a statement setting out the following information:

(i) details of any premises entered, anything opened and any object removed and replaced under the warrant;

(ii) whether the surveillance device was retrieved under the warrant;

(iii) if the device was not retrieved, the reason why;

(iv) details of the compliance with the conditions (if any) to which the warrant was subject;

(e) a statement as to whether each application made by a law enforcement officer of the agency for an emergency authorisation, or for approval of powers exercised under an emergency authorisation, was granted, refused or withdrawn;

(f) details of each use by the agency, or by a law enforcement officer of the agency, of information obtained by the use of a surveillance device by a law enforcement officer of the agency;

(g) details of each communication by a law enforcement officer of the agency to a person other than a law enforcement officer of the agency of information obtained by the use of a surveillance device by a law enforcement officer of the agency;

(h) details of each occasion when, to the knowledge of a law enforcement officer of the agency, information obtained by the use of a surveillance device by a law enforcement officer of the agency was given in evidence in a relevant proceeding;

(i) details of the destruction of records or reports under section 35 (1) (b) (Dealing with records obtained by use of surveillance devices).

41 Register of warrants and emergency authorisations

(1) The chief officer of a law enforcement agency must keep a register of warrants and emergency authorisations.

(2) The register must state, for each warrant issued to a law enforcement officer of the agency—

(a) the date of issue of the warrant; and

(b) the name of the judge or magistrate who issued the warrant; and

(c) the name of the law enforcement officer named in the warrant as the person primarily responsible for executing it; and

(d) the relevant offence in relation to which the warrant was issued; and

(e) the period during which the warrant is in force; and

(f) details of any amendment or extension of the warrant.

(3) The register must state, for each emergency authorisation given to a law enforcement officer of the agency—

(a) the date the emergency authorisation was given; and

(b) the name of the chief officer who gave the emergency authorisation; and

(c) the name of the law enforcement officer to whom the emergency authorisation was given; and

(d) the relevant offence in relation to which the emergency authorisation was given; and

(e) the date when the application for approval of powers exercised under the emergency authorisation was made.

Division 5.3 Inspections

42 Inspection of records by ombudsman

(1) The ombudsman may inspect the records of a law enforcement agency to determine the extent of compliance with this Act by the agency and law enforcement officers of the agency.

(2) For an inspection under this section, the ombudsman—

(a) after notifying the chief officer of the law enforcement agency, may enter at any reasonable time premises occupied by the agency; and

(b) is entitled to have full and free access at all reasonable times to all records of the agency that are relevant to the inspection; and

(c) may require a member of staff of the agency to give the ombudsman any information that the ombudsman considers necessary, being information that is in the member's possession, or to which the member has access, and that is relevant to the inspection.

(3) The chief officer must ensure that members of staff of the agency give the ombudsman any assistance the ombudsman reasonably requires to enable the ombudsman to exercise functions under this section.

(4) The ombudsman must give a written report prepared under the *Annual Reports (Government Agencies) Act 2004* on the results of each inspection under this section in the preceding financial year.

(5) The report must include a report on the comprehensiveness and adequacy of the records of the agency and the cooperation given by the agency in facilitating the inspection by the ombudsman of those records.

(6) The report must not include any information that, if made public, could reasonably be expected to—

(a) endanger a person's safety; or

(b) prejudice an investigation or prosecution; or

(c) compromise any law enforcement agency's operational activities or methodologies.

Division 5.4 General

43 Evidentiary certificates

(1) The chief officer of a law enforcement agency, or a person assisting the officer, may issue a written certificate signed by the officer or person setting out any facts the officer or person considers relevant in relation to—

(a) anything done by a law enforcement officer of the agency, or by a person assisting or providing technical expertise to the officer, in connection with the execution of a warrant or in accordance with an emergency authorisation; or

(b) anything done by a law enforcement officer of the agency in connection with—

(i) the communication by a person to someone else of; or

(ii) the making use of; or

(iii) the making of a record of; or

(iv) the custody of a record of—

information obtained by the use of a surveillance device under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation.

(2) A document purporting to be a certificate issued under subsection (1) or under a provision of a corresponding law that corresponds to subsection (1) is admissible in evidence in any proceeding.

(3) Subsection (2) does not apply to a certificate to the extent that the certificate sets out facts in relation to anything done in accordance with an emergency authorisation or corresponding emergency authorisation unless the use of powers under that authorisation has been approved under section 29 (Judge may approve emergency use of powers) or under a provision of a corresponding law that corresponds to section 29.

Part 6 Miscellaneous

44 Delegation

(1) Except as provided by this section, and despite any other Act or law to the contrary, the functions of a chief officer under this Act must not be delegated to any other person.

(2) A chief officer may delegate to a senior officer of the law enforcement agency any of the chief officer's functions under this Act.

(3) In this section:

senior officer means a person for the time being holding office as—

(a) in relation to the Australian Federal Police—a police officer of the rank of commander (or a higher rank); or

(b) in relation to the Australian Crime Commission, any of the following:

(i) the Director National Operations;

(ii) a Director;

(iii) an office of the Australian Crime Commission that is prescribed by regulation; or

(c) in relation to the integrity commission—a position of the integrity commission prescribed by regulation.

45 Regulation-making power

(1) The Executive may make regulations for this Act.

Note A regulation must be notified, and presented to the Legislative Assembly, under the Legislation Act.

(2) A regulation may create offences and fix maximum penalties of not more than 10 penalty units for the offences.

Dictionary

(see s 3)

Note 1 The Legislation Act contains definitions and other provisions relevant to this Act.

Note 2 For example, the Legislation Act, dict, pt 1, defines the following terms:

- ACT
- Commonwealth
- coroner
- function
- in relation to
- integrity commission
- integrity commissioner
- judge
- Legislative Assembly
- magistrate
- territory law
- working day.

applicant, for a warrant, means the law enforcement officer who applies, or on whose behalf an application is made, for the warrant.

Australian Crime Commission means the Australian Crime Commission established by the *Australian Crime Commission Act 2002* (Cwlth).

chief officer means—

(a) in relation to the Australian Federal Police—the chief police officer; and

(b) in relation to the Australian Crime Commission—the chief executive officer of the Australian Crime Commission; and

(c) in relation to the integrity commission—the integrity commissioner.

computer means an electronic device for storing or processing information.

corresponding emergency authorisation means an authorisation given under the provisions of a corresponding law that correspond to part 3 (Emergency authorisations).

corresponding law means a law of another jurisdiction that corresponds to this Act, and includes a law of another jurisdiction that is declared by regulation to correspond to this Act.

corresponding warrant means a warrant issued under the provisions of a corresponding law that correspond to part 2 (Warrants).

corrupt conduct—see the *Integrity Commission Act 2018*, dictionary.

data surveillance device—

(a) means a device or program capable of being used to record or monitor the input of information into or the output of information from a computer; but

(b) does not include an optical surveillance device.

device includes instrument, apparatus and equipment.

disciplinary proceeding means a proceeding of a disciplinary nature under a law of any jurisdiction or of the Commonwealth.

emergency authorisation means an emergency authorisation given under part 3 (Emergency authorisations).

enhancement equipment, in relation to a surveillance device, means equipment capable of enhancing a signal, image or other information obtained by the use of the surveillance device.

install includes attach.

judge includes the associate judge.

jurisdiction means a State or Territory of the Commonwealth.

law enforcement agency means—

(a) the Australian Federal Police; or

(b) the Australian Crime Commission; or

(c) the integrity commission.

law enforcement officer—

(a) means—

(i) a police officer; or

(ii) a member of staff of the Australian Crime Commission; or

(iii) an investigator under the *Integrity Commission Act 2018*; and

(b) includes a person who is seconded to a law enforcement agency, including (but not limited to) a member of the police force or police service, and a police officer (however described), of another jurisdiction.

listening device—

(a) means a device capable of being used to overhear, record, monitor or listen to a conversation or words spoken to or by any person in conversation; but

(b) does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit that person to hear only sounds ordinarily audible to the human ear.

maintain, in relation to a surveillance device, includes—

(a) adjust, relocate, repair or service the device; and

(b) replace a faulty device.

optical surveillance device—

(a) means a device capable of being used to record visually or observe an activity; but

(b) does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.

participating jurisdiction means a jurisdiction in which a corresponding law is in force.

premises includes the following, whether in or outside the ACT:

(a) land;

(b) a building or vehicle;

(c) a part of a building or vehicle;

(d) any place, whether built on or not.

protected information, for division 5.1 (Restrictions on use, communication and publication of information)—see section 33.

public officer—

(a) means—

(i) a person employed by, or holding an office established under a law of, the Territory; or

(ii) a person employed by a territory authority; and

(b) includes a law enforcement officer.

record includes the following:

(a) an audio, visual or audiovisual record;

(b) a record in digital form;

(c) a documentary record prepared from a record mentioned in paragraph (a) or (b).

relevant offence means—

(a) an offence against an ACT law punishable by imprisonment of 3 years or more; or

(b) an offence against an ACT law prescribed by regulation.

relevant proceeding means any of the following:

(a) the prosecution of a relevant offence;

(b) a proceeding for the confiscation, forfeiture or restraint of property or for the imposition of a pecuniary penalty in connection with a relevant offence;

(c) a proceeding for the protection of a child or intellectually impaired person;

(d) a proceeding concerning the validity of a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation;

(e) a disciplinary proceeding against a public officer;

(f) an examination before the integrity commission;

(g) a coronial inquest or inquiry if, in the opinion of the coroner, the event that is the subject of the inquest or inquiry may have resulted from the commission of a relevant offence;

(h) a proceeding under the *Mutual Assistance in Criminal Matters Act 1987* (Cwlth), section 13 in relation to a criminal matter that concerns an offence—

(i) against the laws of the foreign country that made the request resulting in the proceeding; and

(ii) punishable by imprisonment of 3 years or more.

(i) a proceeding for the taking of evidence under the *Extradition Act 1988* (Cwlth), section 43 to the extent that the proceeding relates to a relevant offence;

(j) a proceeding for the extradition of a person from another jurisdiction to the ACT, to the extent that the proceeding relates to a relevant offence;

(k) a proceeding under the *International War Crimes Tribunals Act 1995* (Cwlth), part 4.1;

(l) a proceeding of the International Criminal Court.

remote application for a warrant, means an application mentioned in section 12 or section 20.

report, of a conversation or activity, includes a report of the substance, meaning or purport of the conversation or activity.

retrieval warrant means a warrant issued under division 2.3 (Retrieval warrants).

surveillance device means—

(a) a data surveillance device, a listening device, an optical surveillance device or a tracking device; or

(b) a device that is a combination of any 2 or more of the devices mentioned in paragraph (a); or

(c) a device of a kind prescribed by regulation.

surveillance device warrant means a warrant issued under division 2.2 (Surveillance device warrants) or under section 29 (3) (Judge may approve emergency use of powers).

tracking device means an electronic device capable of being used to work out or monitor the location of a person or an object or the status of an object.

unsworn application, for a warrant, means an application under section 11 (4) or section 19 (4).

use, of a surveillance device, includes use of the device to record a conversation or other activity.

vehicle includes aircraft and vessel.

warrant means surveillance device warrant or retrieval warrant.

Endnotes

1 About the endnotes

Amending and modifying laws are annotated in the legislation history and the amendment history. Current modifications are not included in the republished law but are set out in the endnotes.

Not all editorial amendments made under the *Legislation Act 2001*, part 11.3 are annotated in the amendment history. Full details of any amendments can be obtained from the Parliamentary Counsel's Office.

Uncommenced amending laws are not included in the republished law. The details of these laws are underlined in the legislation history. Uncommenced expiries are underlined in the legislation history and amendment history.

If all the provisions of the law have been renumbered, a table of renumbered provisions gives details of previous and current numbering.

The endnotes also include a table of earlier republications.

2 Abbreviation key

A = Act
AF = Approved form
am = amended
amdt = amendment
AR = Assembly resolution
ch = chapter
CN = Commencement notice
def = definition
DI = Disallowable instrument
dict = dictionary
disallowed = disallowed by the Legislative Assembly
div = division
exp = expires/expired
Gaz = gazette
hdg = heading
IA = Interpretation Act 1967
ins = inserted/added
LA = Legislation Act 2001
LR = legislation register
LRA = Legislation (Republication) Act 1996
mod = modified/modification
NI = Notifiable instrument
o = order
om = omitted/repealed
ord = ordinance
orig = original
par = paragraph/subparagraph
pres = present
prev = previous
(prev...) = previously
pt = part
r = rule/subrule
reloc = relocated
renum = renumbered
R[X] = Republication No
RI = reissue
s = section/subsection
sch = schedule
sdiv = subdivision
SL = Subordinate law
sub = substituted
underlining = whole or part not commenced or to be expired

3 Legislation history

Crimes (Surveillance Devices) Act 2010 A2010-23
notified LR 7 July 2010
s 1, s 2 commenced 7 July 2010 (LA s 75 (1))
remainder commenced 7 January 2011 (s 2 and LA s 79)

as amended by

Statute Law Amendment Act 2014 A2014-18 sch 3 pt 3.7
notified LR 20 May 2014
s 1, s 2 commenced 20 May 2014 (LA s 75 (1))
sch 3 pt 3.7 commenced 10 June 2014 (s 2 (1))

Justice and Community Safety Legislation Amendment Act 2014 (No 2) A2014-49 sch 1 pt 1.6
notified LR 10 November 2014
s 1, s 2 commenced 10 November 2014 (LA s 75 (1))
sch 1 pt 1.6 commenced 17 November 2014 (s 2)

Crimes Legislation Amendment Act 2015 A2015-3 pt 7
notified LR 2 March 2015
s 1, s 2 commenced 2 March 2015 (LA s 75 (1))
pt 7 commenced 3 March 2015 (s 2 (1))

Freedom of Information Act 2016 A2016-55 sch 4 pt 4.8 (as am by A2017-14 s 19)
notified LR 26 August 2016
s 1, s 2 commenced 26 August 2016 (LA s 75 (1))
sch 4 pt 4.8 commenced 1 January 2018 (s 2 as am by A2017-14 s 19)

Justice and Community Safety Legislation Amendment Act 2017 (No 2) A2017-14 s 19
notified LR 17 May 2017
s 1, s 2 commenced 17 May 2017 (LA s 75 (1))
s 19 commenced 24 May 2017 (s 2 (1))

Note This Act only amends the Freedom of Information Act 2016 A2016-55.

Crimes Legislation Amendment Act 2018 (No 2) A2018-40 pt 5

notified LR 7 November 2018

s 1, s 2 commenced 7 November 2018 (LA s 75 (1))

pt 5 commenced 8 November 2018 (s 2)

Integrity Commission Act 2018 A2018-52 sch 1 pt 1.8 (as am by A2019-18 s 4)

notified LR 11 December 2018

s 1, s 2 commenced 11 December 2018 (LA s 75 (1))

sch 1 pt 1.8 commenced 1 December 2019 (s 2 (2) (a) as am by A2019-18 s 4)

Integrity Commission Amendment Act 2019 A2019-18 s 4

notified LR 14 June 2019

s 1, s 2 commenced 14 June 2019 (LA s 75 (1))

s 3, s 4 commenced 15 June 2019 (s 2 (1))

Note This Act only amends the Integrity Commission Act 2018 A2018-52.

Crimes Legislation Amendment Act 2021 (No 2) A2021-18 pt 4

notified LR 11 August 2021

s 1, s 2 commenced 11 August 2021 (LA s 75 (1))

pt 4 awaiting commencement

Justice and Community Safety Legislation Amendment Act 2021 (No 2) A2021-33 pt 7

notified LR 10 December 2021

s 1, s 2 commenced 10 December 2021 (LA s 75 (1))

pt 7 commenced 17 December 2021 (s 2 (1))

4 Amendment history

Commencement
s 2 om LA s 89 (4)

Purposes of Act
s 6 am A2018-52 amdt 1.55

Relationship to other laws and matters
s 7 am A2016-55 amdt 4.10

Investigation taken to be conducted in ACT
s 8 am A2018-52 amdt 1.56

Who may issue warrants?
s 10 am A2018-40 s 15

Surveillance device warrant—application
s 11 am A2018-52 amdts 1.57-1.59

Surveillance device warrant—deciding the application
s 13 am A2018-52 amdt 1.60

What must a surveillance device warrant contain?
s 14 am A2018-52 amdt 1.61

Extension and amendment of surveillance device warrant
s 16 am A2014-18 amdt 3.28, amdt 3.29

Discontinuance of use of surveillance device under warrant
s 18 am A2018-52 amdt 1.62

What must a retrieval warrant contain?
s 22 am A2015-3 s 30

Application of pt 3—integrity commission
s 24A ins A2018-52 amdt 1.63

Prohibition on communication or publication of protected information
s 34 am A2014-49 amdt 1.13; A2018-52 amdt 1.64; pars renum R7 LA

Protection of surveillance device technologies and methods
s 36 am A2018-52 amdt 1.65

Delegation
s 44 am A2018-52 amdt 1.66; A2021-33 s 15

Dictionary

dict	am A2014-18 amdt 3.30; A2018-52 amdt 1.67
	def ***chief officer*** am A2018-52 amdt 1.68
	def ***corrupt conduct*** ins A2018-52 amdt 1.69
	def ***judge*** ins A2018-40 s 16
	def ***law enforcement agency*** am A2018-52 amdt 1.70
	def ***law enforcement officer*** am A2018-52 amdt 1.71
	def ***relevant proceeding*** am A2018-52 amdt 1.72; pars renum R7 LA
	def ***unsworn application*** sub A2014-18 amdt 3.31

5 Earlier republications

Some earlier republications were not numbered. The number in column 1 refers to the publication order.

Since 12 September 2001 every authorised republication has been published in electronic pdf format on the ACT legislation register. A selection of authorised republications have also been published in printed format. These republications are marked with an asterisk (*) in column 1. Electronic and printed versions of an authorised republication are identical.

Republication No and date	Effective	Last amendment made by	Republication for
R1 7 Jan 2011	7 Jan 2011– 9 June 2014	not amended	new Act
R2 10 June 2014	10 June 2014– 16 Nov 2014	A2014-18	amendments by A2014-18
R3 17 Nov 2014	17 Nov 2014- 2 Mar 2015	A2014-49	amendments by A2014-49
R4 3 Mar 2015	3 Mar 2015- 31 Dec 2017	A2015-3	amendments by A2015-3
R5 1 Jan 2018	1 Jan 2018– 7 Nov 2018	A2017-14	amendments by A2016-55 as amended by A2017-14
R6 8 Nov 2018	8 Nov 2018– 30 Nov 2019	A2018-40	amendments by A2018-40
R7 1 Dec 2019	1 Dec 2019– 16 Dec 2021	A2019-18	amendments by A2018-52 as amended by A2019-18