Surveillance Devices Act 2004

No. 152, 2004

Compilation No. 59

Compilation date: 8 November 2025

Includes amendments: Act No. 60, 2025

Prepared by the Office of Parliamentary Counsel, Canberra

Authorised Version C2025C00651 registered 28/11/2025

About this compilation

This compilation

This is a compilation of the *Surveillance Devices Act 2004* that shows the text of the law as amended and in force on 8 November 2025 (the ***compilation date***).

The notes at the end of this compilation (the ***endnotes***) include information about amending laws and the amendment history of provisions of the compiled law.

Uncommenced amendments

The effect of uncommenced amendments is not shown in the text of the compiled law. The details of amendments made up to, but not commenced at, the compilation date are underlined in the endnotes. Any uncommenced amendments affecting the law are accessible on the Register (www.legislation.gov.au).

Application, saving and transitional provisions

If the operation of a provision or amendment of the compiled law is affected by an application, saving or transitional provision that is not included in this compilation, details are included in the endnotes.

Editorial changes

For more information about any editorial changes made in this compilation, see the endnotes.

Presentational changes

The *Legislation Act 2003* provides for First Parliamentary Counsel to make presentational changes to a compilation. Presentational changes are applied to give a more consistent look and feel to legislation published on the Register, and enable the user to more easily navigate those documents.

Modifications

If the compiled law is modified by another law, the compiled law operates as modified but the modification does not amend the text of the law. Accordingly, this compilation does not show the text of the compiled law as modified. Any modifications affecting the law are accessible on the Register.

Self-repealing provisions

If a provision of the compiled law has been repealed in accordance with a provision of the law, details are included in the endnotes.

Contents

Part 1—Preliminary 1

1 Short title....1
2 Commencement....1
3 Purposes....1
4 Relationship to other laws and matters....4
5 Schedule(s)....6
6 Definitions....6
6A Law enforcement agencies....23
6B Authorisation of law enforcement officer....29
6C When a Part 5.3 supervisory order is taken to be in force....29
6D Succeeding Part 5.3 supervisory orders....29
6E When a community safety supervision order is taken to be in force....30
6F Succeeding community safety supervision order....30
7 State offence that has a federal aspect....30
7A Criminal network of individuals....31
8 External Territories....32
9 Binding the Crown....32

Part 2—Warrants 33

Division 1—Introduction 33

10 Types of warrant....33
11 Who may issue etc. warrants?....33
12 Eligible Judges....34
13 Nominated ART members....35

Division 2—Surveillance device warrants 36

14 Application for surveillance device warrant....36
15 Remote application....40
16 Determining the application....41
17 What must a surveillance device warrant contain?....45
18 What a surveillance device warrant authorises....48
19 Extension and variation of surveillance device warrant....51
20 Revocation of surveillance device warrant....51
21 Discontinuance of use of surveillance device under warrant....52

Division 3—Retrieval warrants 55

22 Application for retrieval warrant....55

Authorised Version C2025C00651 registered 28/11/2025

23 Remote application 56
24 Determining the application....56
25 What must a retrieval warrant contain? 57
26 What a retrieval warrant authorises 57
27 Revocation of retrieval warrant 58

Division 4—Computer access warrants 60

27A Application for computer access warrant 60
27B Remote application 66
27C Determining the application....66
27D What must a computer access warrant contain? 71
27E What a computer access warrant authorises 74
27F Extension and variation of computer access warrant....79
27G Revocation of computer access warrant 80
27H Discontinuance of access under warrant....80
27J Relationship of this Division to parliamentary privileges and immunities 83

Division 5—Data disruption warrants 84

27KAA Sunsetting 84
27KA Application for data disruption warrant....84
27KB Remote application 86
27KBA Endorsement of application—Australian Federal Police....86
27KBB Endorsement of application—Australian Crime Commission 87
27KC Determining the application....89
27KD What must a data disruption warrant contain?....92
27KE What a data disruption warrant authorises....94
27KF Extension and variation of data disruption warrant 99
27KG Revocation of data disruption warrant....100
27KH Discontinuance of access and disruption under warrant....100
27KJ Relationship of this Division to parliamentary privileges and immunities 101

Division 6—Network activity warrants 102

27KKA Sunsetting 102
27KK Application for network activity warrant....102
27KL Remote application 104
27KM Determining the application....104
27KN What must a network activity warrant contain? 107
27KP What a network activity warrant authorises 109
27KQ Extension and variation of network activity warrant....113

Authorised Version C2025C00651 registered 28/11/2025

27KR Revocation of network activity warrant....114
27KS Discontinuance of access under warrant....116
27KT Relationship of this Division to parliamentary privileges and immunities....117

Part 3—Emergency authorisations 118

27KU Sunsetting—emergency authorisation for disruption of data held in a computer....118
28 Emergency authorisation—serious risks to person or property....118
29 Emergency authorisation—urgent circumstances relating to recovery order....121
30 Emergency authorisation—risk of loss of evidence....122
31 Record of emergency authorisations to be made....125
32 Attributes of emergency authorisations....125
33 Application for approval of emergency authorisation....126
34 Consideration of application....127
35 Judge or nominated ART member may approve giving of an emergency authorisation for the use of a surveillance device....131
35A Judge or nominated ART member may approve giving of an emergency authorisation for access to data held in a computer....133
35B Judge or nominated ART member may approve giving of an emergency authorisation for disruption of data held in a computer....135
36 Admissibility of evidence....136
36A Relationship of this Part to parliamentary privileges and immunities....137

Part 4—Use of certain surveillance devices without warrant 138

37 Use of optical surveillance devices without warrant....138
38 Use of surveillance devices without warrant for listening to or recording words in limited circumstances....139
39 Use and retrieval of tracking devices without warrant in certain circumstances....144
40 Record of tracking device authorisations to be kept....147

Part 5—Extraterritorial operation of warrants 149

41 Definitions....149
42 Extraterritorial operation of surveillance device warrants....149
43 Evidence obtained from extraterritorial surveillance not to be tendered in evidence unless court satisfied properly obtained....152

Authorised Version C2025C00651 registered 28/11/2025

43A Extraterritorial operation of computer access warrants 152
43B Evidence obtained from extraterritorial computer access not to be tendered in evidence unless court satisfied properly obtained....156
43C Extraterritorial operation of data disruption warrants....156
43D Evidence obtained from extraterritorial computer access not to be tendered in evidence unless court is satisfied that the evidence was properly obtained....159
43E Extraterritorial operation of network activity warrants 160

Part 6—Compliance and monitoring 163

Division 1—Restrictions on use, communication and publication of information 163

44 What is protected information?....163
44A What is protected network activity warrant information? 165
45 Prohibition on use, recording, communication or publication of protected information or its admission in evidence....166
45A Protected information related to integrity operations 174
45B Prohibition on use, recording, communication or publication of protected network activity warrant information or its admission in evidence....175
46 Dealing with records obtained by using a surveillance device or accessing data held in a computer 181
46AA Dealing with records obtained by accessing data under a network activity warrant 182
46A Destruction of records—information obtained before a Part 5.3 supervisory order came into force 184
46B Destruction of records—information obtained before a community safety supervision order came into force 185
47 Protection of surveillance device technologies and methods 187
47A Protection of computer access technologies and methods....188
47B Protection of data disruption technologies and methods 189
48 Protected information in the custody of a court, tribunal or Royal Commission....191

Division 2—Reporting and record-keeping 192

49 Report on each warrant or authorisation....192
49A Notification to Ombudsman in relation to Part 5.3 warrants or Part 9.10 warrants....199
49B Notification to Ombudsman in relation to concealment of access under a computer access warrant....200

Authorised Version C2025C00651 registered 28/11/2025

49C Notification to Ombudsman of things done under a data disruption warrant 200
49D Notification to Inspector-General of Intelligence and Security of things done under a network activity warrant 201
50 Annual reports 202
50A Deferral of inclusion of information in annual report 205
51 Keeping documents connected with warrants, emergency authorisations and tracking device authorisations 207
52 Other records to be kept 208
53 Register of warrants, emergency authorisations and tracking device authorisations 210

Division 3—Inspections 213

54 Appointment of inspecting officers 213
55 Inspection of records 213
56 Power to obtain relevant information 215
57 Ombudsman to be given information and access despite other laws 216
58 Exchange of information between Ombudsman and State inspecting authorities 217
59 Delegation by Ombudsman 218
60 Ombudsman not to be sued 218
61 Report on inspection 218
61A Report may cover notified breaches in relation to Part 5.3 warrants or Part 9.10 warrants 220

Division 4—General 221

62 Evidentiary certificates 221

Part 7—Miscellaneous 224

63 Delegation by chief officer of law enforcement agency 224
64 Compensation for loss or injury 224
64A Person with knowledge of a computer or a computer system to assist access etc. 226
64B Person with knowledge of a computer or a computer system to assist disruption of data etc. 235
65 Minor defects in connection with warrant or other authority 240
65A Protection of persons—control order declared to be void 241
65B Dealing with information obtained under a warrant or authorisation etc.—control order declared to be void 244
65C Evidence obtained from access to, or disruption of, data under a data disruption warrant etc. 247
66 Regulations 247

Authorised Version C2025C00651 registered 28/11/2025

Schedule 1—Amendment of other legislation and transitional and saving provisions 248
Australian Federal Police Act 1979 248
Customs Act 1901 249

Endnotes 251

Endnote 1—About the endnotes 251

Endnote 2—Abbreviation key 253

Endnote 3—Legislation history 254

Endnote 4—Amendment history 262

Authorised Version C2025C00651 registered 28/11/2025

An Act to set out the powers of Commonwealth law enforcement agencies with respect to surveillance devices and access to, and disruption of, data held in computers, and for related purposes

Part 1—Preliminary

1 Short title

This Act may be cited as the *Surveillance Devices Act 2004*.

2 Commencement

This Act commences on the day on which it receives the Royal Assent.

3 Purposes

The main purposes of this Act are:

(a) to establish procedures for law enforcement officers to obtain warrants, emergency authorisations and tracking device authorisations for the installation and use of surveillance devices in relation to criminal investigations and the location and safe recovery of children to whom recovery orders relate; and

(aaa) to establish procedures for law enforcement officers to obtain warrants and emergency authorisations that:

(i) are for access to data held in computers; and

(ii) relate to criminal investigations and the location and safe recovery of children to whom recovery orders relate; and

(aab) to establish procedures for certain law enforcement officers of the Australian Federal Police or the Australian Crime Commission to obtain warrants and emergency authorisations that:

Authorised Version C2025C00651 registered 28/11/2025

(i) authorise the disruption of data held in computers; and

(ii) are likely to substantially assist in frustrating the commission of relevant offences; and

(aac) to establish procedures for the chief officer of the Australian Federal Police or the Australian Crime Commission to obtain warrants that:

(i) authorise access to data held in computers; and

(ii) will substantially assist in the collection of intelligence that relates to criminal networks of individuals; and

(aad) to establish procedures for law enforcement officers to obtain warrants for the installation and use of surveillance devices, or for access to data held in computers, in cases where the use of the device or the access to the data would be likely to assist in determining whether to apply for a post-sentence order; and

(aae) to establish procedures for law enforcement officers to obtain warrants for the installation and use of surveillance devices, or for access to data held in computers, in cases where a Part 5.3 supervisory order is in force, and the use of the device or the access to the data would be likely to substantially assist in:

(i) achieving a Part 5.3 object; or

(ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and

(aaf) to establish procedures for law enforcement officers to obtain tracking device authorisations for the use of tracking devices in cases where a Part 5.3 supervisory order is in force in relation to a person, and the use of a tracking device is to obtain information relating to the person for either of the following purposes:

(i) achieving a Part 5.3 object;

(ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and

Authorised Version C2025C00651 registered 28/11/2025

(aag) to establish procedures for law enforcement officers to obtain warrants for the installation and use of surveillance devices, or for access to data held in computers, in cases where a community safety supervision order is in force, and the use of the device or the access to the data would be likely to substantially assist in:

(i) achieving a Part 9.10 object; or

(ii) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with; and

(aah) to establish procedures for law enforcement officers to obtain tracking device authorisations for the use of tracking devices in cases where a community safety supervision order is in force in relation to a person, and the use of a tracking device is to obtain information relating to the person for either of the following purposes:

(i) achieving a Part 9.10 object;

(ii) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with; and

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

(ba) to restrict the use, communication and publication of information that is obtained through accessing or disrupting data held in computers or that is otherwise connected with computer data access operations or computer data disruption operations; and

(c) to impose requirements for the secure storage and destruction of records, and the making of reports, in connection with surveillance device operations, computer data access operations and computer data disruption operations.

Authorised Version C2025C00651 registered 28/11/2025

4 Relationship to other laws and matters

(1) Except where there is express provision to the contrary, this Act is not intended to affect any other law of the Commonwealth, any law of a State, or any law of a self-governing Territory, that:

(a) prohibits or regulates the use of surveillance devices; or

(b) prohibits or regulates access to data held in computers; or

(c) prohibits or regulates disruption of data held in computers.

(2) For the avoidance of doubt, except where express provision is made to the contrary, nothing in this Act applies to any body, organisation or agency, however described, that is involved in the collection of information or intelligence.

(3) This Act is not intended to 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.

(4) For the avoidance of doubt, it is intended that a warrant may be issued, or an emergency authorisation or tracking device authorisation given, under this Act for the installation, use, maintenance or retrieval of a surveillance device in relation to a relevant offence or a recovery order.

(4A) For the avoidance of doubt, it is intended that a warrant may be issued, or an emergency authorisation given, under this Act:

(a) for access to data held in a computer; and

(b) in relation to a relevant offence or a recovery order.

(4B) For the avoidance of doubt, it is intended that a warrant may be issued, or an emergency authorisation given, under this Act:

(a) for access to, and disruption of, data held in a computer; and

(b) in relation to one or more relevant offences.

(4C) For the avoidance of doubt, it is intended that a warrant may be issued under this Act:

(a) for access to data held in a computer; and

Authorised Version C2025C00651 registered 28/11/2025

(b) in relation to the collection of intelligence that relates to a criminal network of individuals.

(5) To avoid doubt, it is intended that a warrant may be issued under this Act for the installation, use, maintenance or retrieval of a surveillance device, or for access to data held in a computer, if:

(a) consideration is being given, will be given, or is likely to be given, as to whether to apply for a post-sentence order, and the use of the device or the access to the data would be likely to assist in determining whether to apply for the order; or

(b) a Part 5.3 supervisory order is in force, and the use of the device or the access to the data would be likely to substantially assist in:

(i) achieving a Part 5.3 object; or

(ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with.

(6) To avoid doubt, a tracking device authorisation may be given under this Act for the use of a tracking device to obtain information relating to a person if:

(a) a Part 5.3 supervisory order is in force in relation to the person; and

(b) the use is for either of the following purposes:

(i) achieving a Part 5.3 object;

(ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with.

(7) To avoid doubt, it is intended that a warrant may be issued under this Act for the installation, use, maintenance or retrieval of a surveillance device, or for access to data held in a computer, if:

(a) consideration is being given, will be given, or is likely to be given, as to whether to apply for a Part 9.10 order, and the use of the device or the access to the data would be likely to assist in determining whether to apply for the order; or

Authorised Version C2025C00651 registered 28/11/2025

(b) a community safety supervision order is in force, and the use of the device or the access to the data would be likely to substantially assist in:

(i) achieving a Part 9.10 object; or

(ii) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with.

(8) To avoid doubt, a tracking device authorisation may be given under this Act for the use of a tracking device to obtain information relating to a person if:

(a) a community safety supervision order is in force in relation to the person; and

(b) the use is for either of the following purposes:

(i) achieving a Part 9.10 object;

(ii) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with.

5 Schedule(s)

Each Act that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

6 Definitions

(1) In this Act:

AFP Minister has the meaning given by section 100.1 of the *Criminal Code*.

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

appropriate authorising officer:

Authorised Version C2025C00651 registered 28/11/2025

(a) of a law enforcement agency—has the meaning given by subsection 6A(4); or

(b) in relation to a law enforcement officer belonging to or seconded to a law enforcement agency—means an appropriate authorising officer of the law enforcement agency.

Note: See also subsection (4) of this section (persons who belong or are seconded to the Australian Crime Commission or the National Anti-Corruption Commission).

carrier means:

(a) a carrier within the meaning of the *Telecommunications Act 1997*; or

(b) a carriage service provider within the meaning of that Act.

chief officer has the meaning given by subsection 6A(2).

communication in transit means a communication (within the meaning of the *Telecommunications Act 1997*) passing over a telecommunications network (within the meaning of that Act).

community safety detention order has the same meaning as in Division 395 of the *Criminal Code*.

community safety supervision order has the same meaning as in Division 395 of the *Criminal Code*.

computer means all or part of:

(a) one or more computers; or

(b) one or more computer systems; or

(c) one or more computer networks; or

(d) any combination of the above.

computer access warrant means a warrant issued under section 27C or subsection 35A(4) or (5).

confirmed control order has the same meaning as in Part 5.3 of the *Criminal Code*.

Authorised Version C2025C00651 registered 28/11/2025

control order has the same meaning as in Part 5.3 of the *Criminal Code*.

criminal network of individuals has the meaning given by section 7A.

data includes:

(a) information in any form; and

(b) any program (or part of a program).

data disruption intercept information has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

data disruption warrant means a warrant issued under section 27KC or subsection 35B(2) or (3).

data held in a computer includes:

(a) data held in any removable data storage device for the time being held in a computer; and

(b) data held in a data storage device on a computer network of which the computer forms a part.

data storage device means a thing (for example, a disk or file server) containing (whether temporarily or permanently), or designed to contain (whether temporarily or permanently), data for use by a computer.

data surveillance device means any device or program capable of being used to record or monitor the input of information into, or the output of information from, an electronic device for storing or processing information, but does not include an optical surveillance device.

detained in custody in a prison has the meaning given by section 100.1 of the *Criminal Code*.

device includes instrument, apparatus and equipment.

digital currency has the same meaning as in the *A New Tax System (Goods and Services Tax) Act 1999*.

Authorised Version C2025C00651 registered 28/11/2025

disciplinary proceeding:

(a) means a proceeding of a disciplinary nature under a law of the Commonwealth or of a State or Territory; and

(b) includes action taken under Subdivision D of Division 3 of Part V of the *Australian Federal Police Act 1979*.

disrupting data held in a computer means adding, copying, deleting or altering data held in the computer.

Note: This expression is used in the provisions of this Act that relate to:

(a) data disruption warrants; or

(b) emergency authorisations for disruption of data held in a computer.

electronically linked group of individuals means a group of 2 or more individuals, where each individual in the group does, or is likely to do, either or both of the following things:

(a) use the same electronic service as at least one other individual in the group;

(b) communicate with at least one other individual in the group by electronic communication.

electronic communication means a communication of information:

(a) whether in the form of text; or

(b) whether in the form of data; or

(c) whether in the form of speech, music or other sounds; or

(d) whether in the form of visual images (animated or otherwise); or

(e) whether in any other form; or

(f) whether in any combination of forms;

by means of guided and/or unguided electromagnetic energy.

electronic service has the same meaning as in Part 15 of the *Telecommunications Act 1997*.

eligible Judge means an eligible Judge within the meaning of section 12.

Authorised Version C2025C00651 registered 28/11/2025

emergency authorisation means an emergency authorisation given under Part 3.

emergency authorisation for access to data held in a computer means an emergency authorisation given in response to an application under subsection 28(1A), 29(1A) or 30(1A).

emergency authorisation for disruption of data held in a computer means an emergency authorisation given in response to an application under subsection 28(1C).

engage in a hostile activity has the same meaning as in Part 5.3 of the *Criminal Code*.

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.

executive level has the meaning given by subsection 6A(8).

extended supervision order has the meaning given by section 105A.2 of the *Criminal Code*.

federal law enforcement officer means a law enforcement officer mentioned in column 3 of the table in subsection 6A(6).

foreign country, when used in the expression ***hostile activity in a foreign country***, has the same meaning as in the *Criminal Code*.

general computer access intercept information has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

IGIS official means:

(a) the Inspector-General of Intelligence and Security; or

(b) any other person covered by subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*.

Immigration and Border Protection Department means the Department administered by the Minister administering the *Australian Border Force Act 2015*.

Authorised Version C2025C00651 registered 28/11/2025

Immigration Minister means the Minister administering the *Migration Act 1958*.

Independent Commission Against Corruption means the Independent Commission Against Corruption constituted by the *Independent Commission Against Corruption Act 1988* of New South Wales.

inspecting officer means a person appointed by the Ombudsman under section 54 to be an inspecting officer.

install includes attach.

integrity authority means:

(a) an integrity testing controlled operations authority under Part IAB of the *Crimes Act 1914* authorising a controlled operation under that Part; or

(b) an integrity testing authority under Part IABA of the *Crimes Act 1914* authorising an integrity testing operation under that Part.

integrity operation means:

(a) a controlled operation authorised by an integrity testing controlled operation authority granted under Part IAB of the *Crimes Act 1914*; or

(b) an integrity testing operation authorised by an integrity testing authority granted under Part IABA of the *Crimes Act 1914*.

intercepting a communication passing over a telecommunications system has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

interim control order has the same meaning as in Part 5.3 of the *Criminal Code*.

interim supervision order has the meaning given by section 105A.2 of the *Criminal Code*.

international assistance application means:

Authorised Version C2025C00651 registered 28/11/2025

(a) an application for a surveillance device warrant; or

(b) an application for a computer access warrant;

made under an international assistance authorisation.

international assistance authorisation means:

(a) an authorisation under subsection 15CA(1) or 15CC(1) of the *Mutual Assistance in Criminal Matters Act 1987*; or

(b) an authorisation under subsection 79A(1) of the *International Criminal Court Act 2002*; or

(c) an authorisation under subsection 32A(1) of the *International War Crimes Tribunals Act 1995*.

International Criminal Court has the same meaning as ***ICC*** in the *International Criminal Court Act 2002*.

investigative proceeding has the same meaning as in the *Mutual Assistance in Criminal Matters Act 1987*.

law enforcement agency has the meaning given by subsection 6A(1).

law enforcement officer has the meaning given by subsection 6A(3).

listening device means any 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 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.

member of the staff, in relation to the Independent Commission Against Corruption of South Australia, means a person who is engaged under subsection 12(1) of the *Independent Commission Against Corruption Act 2012* (SA).

Authorised Version C2025C00651 registered 28/11/2025

National Anti-Corruption Commission officer means a staff member of the NACC (within the meaning of the *National Anti-Corruption Commission Act 2022*).

network activity warrant means a warrant issued under section 27KM.

network activity warrant intercept information has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

nominated ART member means a person in respect of whom a nomination under section 13 is in force.

offence has a meaning affected by subsection (5).

Ombudsman means the person holding office as the Commonwealth Ombudsman under the *Ombudsman Act 1976*.

Ombudsman official means:

(a) the Ombudsman; or

(b) a Deputy Commonwealth Ombudsman; or

(c) a person who is a member of the staff referred to in subsection 31(1) of the *Ombudsman Act 1976*.

optical surveillance device means any device capable of being used to record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome that impairment.

Part 5.3 information has the meaning given by subsection 50A(6).

Part 5.3 object means:

(a) in relation to a control order—any of the following:

(i) the protection of the public from a terrorist act;

(ii) the prevention of the provision of support for, or the facilitation of, a terrorist act;

(iii) the prevention of the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or

Authorised Version C2025C00651 registered 28/11/2025

(b) in relation to an extended supervision order or interim supervision order in relation to a person—the protection of the community from the unacceptable risk of the person committing a serious Part 5.3 or 5.3A offence.

Part 5.3 supervisory order means:

(a) a control order; or

(b) an extended supervision order or an interim supervision order.

Note: In Part 5.3 of the *Criminal Code*, a control order means an interim control order or a confirmed control order (see subsection 100.1(1) of the *Criminal Code*).

Part 5.3 warrant means a surveillance device warrant or computer access warrant:

(a) issued to determine whether to apply for a post-sentence order; or

(b) issued in relation to a Part 5.3 supervisory order that is or was in force.

Part 9.10 information has the meaning given by subsection 50A(6).

Part 9.10 object means the protection of the community from serious harm by addressing the unacceptable risk of a serious offender committing a serious violent or sexual offence.

Part 9.10 order means a community safety detention order or a community safety supervision order.

Part 9.10 warrant means a surveillance device warrant or computer access warrant:

(a) issued to determine whether to apply for a Part 9.10 order; or

(b) issued in relation to a community safety supervision order that is or was in force.

post-sentence detention law means any of the following laws:

(a) Part 3 of the *Terrorism (High Risk Offenders) Act 2017* (NSW);

Authorised Version C2025C00651 registered 28/11/2025

(b) Parts 5 and 6 of the *Serious Offenders Act 2018* (Vic.);
(c) Part 3 of the *Criminal Law (High Risk Offenders) Act 2015* (SA);
(d) any other law, or part of a law, of a State or Territory prescribed by the regulations.

post-sentence order means a continuing detention order, an interim detention order, an extended supervision order, or an interim supervision order, under Division 105A of the *Criminal Code*.

post-sentence supervision law means any of the following laws:
(a) Part 2 of the *Terrorism (High Risk Offenders) Act 2017* (NSW);
(b) Parts 3 and 4 of the *Serious Offenders Act 2018* (Vic.);
(c) Part 2 of the *Criminal Law (High Risk Offenders) Act 2015* (SA);
(d) any other law, or part of a law, of a State or Territory prescribed by the regulations.

premises includes:
(a) land; and
(b) a building or vehicle; and
(c) a part of a building or vehicle; and
(d) any place, whether built on or not;
whether within or beyond Australia.

preventative detention order law means:
(a) Division 105 of the *Criminal Code*; or
(b) Part 2A of the *Terrorism (Police Powers) Act 2002* (NSW); or
(c) Part 2A of the *Terrorism (Community Protection) Act 2003* (Vic.); or
(d) the *Terrorism (Preventative Detention) Act 2005* (Qld); or
(e) the *Terrorism (Preventative Detention) Act 2006* (WA); or
(f) the *Terrorism (Preventative Detention) Act 2005* (SA); or
(g) the *Terrorism (Preventative Detention) Act 2005* (Tas.); or

Authorised Version C2025C00651 registered 28/11/2025

(h) Part 2 of the *Terrorism (Extraordinary Temporary Powers) Act 2006* (ACT); or

(i) Part 2B of the *Terrorism (Emergency Powers) Act 2003* (NT).

prosecution, in relation to a criminal offence, includes all stages in the prosecution of that offence, including a committal hearing.

protected information has the meaning given in section 44.

protected network activity warrant information has the meaning given by section 44A.

public officer means a person employed by, or holding an office established by or under a law of, the Commonwealth, a State or a Territory or a person employed by a public authority of the Commonwealth, a State or a Territory.

record includes:

(a) an audio, visual or audio-visual record; and

(b) a record in digital form; and

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

recovery order means:

(a) an order under section 67U of the *Family Law Act 1975*; or

(b) an order for a warrant for the apprehension or detention of a child under subregulation 15(1) or 25(4) of the *Family Law (Child Abduction Convention) Regulations 1986*.

relevant offence means:

(a) an offence against the law of the Commonwealth that is punishable by a maximum term of imprisonment of 3 years or more or for life; or

(b) an offence against a law of a State that has a federal aspect and that is punishable by a maximum term of imprisonment of 3 years or more or for life; or

(c) an offence against section 15 of the repealed *Financial Transaction Reports Act 1988*; or

Authorised Version C2025C00651 registered 28/11/2025

(ca) an offence against section 53, former section 59 or section 139, 140 or 141 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*; or

(d) an offence against section 100, 100A, 100B, 101, 101A or 101AA of the *Fisheries Management Act 1991*; or

(da) an offence against section 46A, 46C, 46D, 49A or 51A of the *Torres Strait Fisheries Act 1984*; or

(db) if a surveillance device warrant, a computer access warrant, or a tracking device authorisation, is issued or given (or is sought) for the purposes of an integrity operation in relation to a suspected offence against the law of the Commonwealth, or of a State or Territory, that is punishable by a maximum term of imprisonment of 12 months or more or for life—that offence; or

(e) an offence that is prescribed by the regulations.

relevant proceeding means:

(a) the prosecution of a relevant offence; or

(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, and any related proceeding; or

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

(d) a proceeding concerning the validity of a warrant, an emergency authorisation or a tracking device authorisation; or

(e) a disciplinary proceeding against a public officer; or

(f) 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; or

(g) a proceeding under subsection 13(2) of the *Mutual Assistance in Criminal Matters Act 1987* in relation to a criminal matter that concerns an offence against the laws of the foreign country that made the request resulting in the proceeding, being an offence punishable by a maximum term of

Authorised Version C2025C00651 registered 28/11/2025

imprisonment of 3 years or more, by imprisonment for life or by the death penalty; or

(h) the authorisation, under section 13A of the *Mutual Assistance in Criminal Matters Act 1987*, of material to be made available to a foreign country for use in the investigation into, or proceedings in relation to, an offence against the laws of that country; or

(i) proceedings for an order under section 67X of the *Family Law Act 1975*; or

(j) a proceeding for the taking of evidence under section 43 of the *Extradition Act 1988*, in so far as the proceeding relates to a relevant offence; or

(k) a proceeding under Division 1 of Part 4 of the *International War Crimes Tribunals Act 1995*; or

(l) a proceeding of the International Criminal Court; or

(m) a proceeding by way of a bail application that relates to a prosecution for a relevant offence; or

(n) a proceeding for review of a decision to refuse such a bail application; or

(o) a proceeding for review of a decision to grant such a bail application; or

(oa) a proceeding under, or related to a matter arising under, Division 105A of the *Criminal Code* (post-sentence orders) or Division 395 of the *Criminal Code* (community safety orders); or

(p) a proceeding in relation to an application under subsection 34B(1) of the *Australian Crime Commission Act 2002* in respect of contempt of the Australian Crime Commission; or

(q) a proceeding under, or a proceeding relating to a matter arising under, Division 104 of the *Criminal Code* (Control orders); or

(r) a proceeding under, or a proceeding relating to a matter arising under, a preventative detention order law, so far as the proceeding relates to a preventative detention order (within the meaning of that preventative detention order law); or

Authorised Version C2025C00651 registered 28/11/2025

(s) a proceeding under, or a proceeding relating to a matter arising under, a post-sentence detention law or a post-sentence supervision law.

remote application for a warrant means an application referred to in section 15, 23, 27B, 27KB or 27KL.

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 3 of Part 2.

serious offender has the same meaning as in Division 395 of the *Criminal Code*.

serious Part 5.3 or 5.3A offence has the meaning given by section 105A.2 of the *Criminal Code*.

serious violent or sexual offence has the same meaning as in Division 395 of the *Criminal Code*.

State offence that has a federal aspect has the meaning given by section 7.

State or Territory law enforcement officer means a law enforcement officer mentioned in column 3 of the table in subsection 6A(7).

succeeding community safety supervision order has the meaning given by section 6F.

succeeding Part 5.3 supervisory order has the meaning given by section 6D.

superior Court Judge means:

(a) a Judge of the Federal Court of Australia; or

(b) a Judge of the Federal Circuit and Family Court of Australia (Division 1).

surveillance device means:

Authorised Version C2025C00651 registered 28/11/2025

(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 referred to in paragraph (a); or
(c) a device of a kind prescribed by the regulations.

surveillance device warrant means a warrant issued under Division 2 of Part 2 or under subsection 35(4) or (5).

sworn includes affirmed.

target agency means any of the following:
(a) the Australian Federal Police;
(b) the Australian Crime Commission;
(c) the Immigration and Border Protection Department;
(d) any other Commonwealth agency (within the meaning of the *National Anti-Corruption Commission Act 2022*).

telecommunications facility means a facility within the meaning of the *Telecommunications Act 1997*.

terrorist act has the same meaning as in the *Crimes Act 1914*.

terrorist offender has the meaning given by section 105A.2 of the *Criminal Code*.

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

tracking device authorisation means a permission given under section 39 by an appropriate authorising officer for a law enforcement officer to use or retrieve a tracking device without a warrant.

unsworn application for a warrant means an application referred to in subsections 14(6) and (7), 22(4) and (5), 27A(9) and (10), 27A(11) and (12), 27A(13), (13A) and (14), 27KA(4) and (5) or 27KK(5) and (6).

Authorised Version C2025C00651 registered 28/11/2025

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

vehicle includes aircraft and vessel.

War Crimes Tribunal has the same meaning as ***Tribunal*** in the *International War Crimes Tribunals Act 1995*.

warrant means:

(a) a surveillance device warrant; or

(b) a retrieval warrant; or

(c) a computer access warrant; or

(d) a data disruption warrant; or

(e) a network activity warrant.

(2) In this Act, a reference to the law enforcement officer primarily responsible for executing a warrant, emergency authorisation or tracking device authorisation is, subject to subsection (3), a reference to:

(a) the person named in the warrant or authorisation as such a person; or

(b) if there is no such person named—the person nominated as such a person by the chief officer of the agency concerned;

whether or not that person is physically present for any step in the execution of the warrant or authorisation.

(3) If the chief officer of a law enforcement agency becomes satisfied that a law enforcement officer of the agency who is, under subsection (2) or under a previous operation of this subsection, the law enforcement officer primarily responsible for executing a warrant, emergency authorisation or tracking device authorisation, ceases, for any reason, to have responsibility for executing the warrant or authorisation:

(a) the chief officer may, by instrument in writing, nominate another person as the law enforcement officer primarily responsible for executing the warrant or authorisation; and

(b) with effect from the execution of the instrument or such later time as is specified in the instrument, that other person

Authorised Version C2025C00651 registered 28/11/2025

becomes the law enforcement officer primarily responsible for executing the warrant or authorisation.

(4) In this Act:

(a) a reference to a person who belongs or is seconded to a law enforcement agency, in the case of the Australian Crime Commission, is a reference to any person who is covered by a paragraph of the definition of ***member of the staff of the ACC*** in section 4 of the *Australian Crime Commission Act 2002*; and

(b) a reference to a person who belongs or is seconded to the Australian Crime Commission is to be similarly construed; and

(c) a reference to a person who belongs or is seconded to a law enforcement agency, in the case of the National Anti-Corruption Commission, is a reference to a National Anti-Corruption Commission officer; and

(d) a reference to a person who belongs or is seconded to the National Anti-Corruption Commission is to be similarly construed.

(5) To avoid doubt, a reference in this Act to an offence in relation to:

(a) an international assistance authorisation that is an authorisation under subsection 79A(1) of the *International Criminal Court Act 2002*; or

(b) an international assistance application that is related to such an authorisation;

is a reference to a crime within the jurisdiction of the ICC (within the meaning of that Act).

Authorised Version C2025C00651 registered 28/11/2025

6A Law enforcement agencies

(1) A body or officer mentioned in an item of column 1 of the table in subsection (6) or (7) is a ***law enforcement agency***.

(2) The ***chief officer***, of the law enforcement agency, is the person mentioned in column 2 of the item.

(3) A ***law enforcement officer***, in relation to the law enforcement agency, is a person mentioned in column 3 of the item.

(4) An ***appropriate authorising officer***, of the law enforcement agency, is a person mentioned in column 4 of the item.

(5) The chief officer of the law enforcement agency may authorise, in writing, a person to be an appropriate authorising officer of the agency if column 4 of the item so provides.

(6) This table deals with federal law enforcement agencies:

Federal law enforcement agencies

	Column 1	Column 2	Column 3	Column 4
	Law enforcement agency	**Chief officer**	**Law enforcement officer**	**Appropriate authorising officer**
5	Australian Federal Police	the Commissioner of Police	(a) the Commissioner of Police; or (b) a Deputy Commissioner of Police; or (c) an AFP employee (within the meaning of the *Australian Federal Police Act 1979*); or (d) a special	(a) the Commissioner of Police; or (b) a Deputy Commissioner of Police; or (c) a senior executive AFP employee the chief officer authorises under subsection (5)

Authorised Version C2025C00651 registered 28/11/2025

Federal law enforcement agencies				
	Column 1	**Column 2**	**Column 3**	**Column 4**
	Law enforcement agency	**Chief officer**	**Law enforcement officer**	**Appropriate authorising officer**
			member; or (e) a person seconded to the Australian Federal Police	
10	National Anti-Corruption Commission	the National Anti-Corruption Commissioner	(a) the National Anti-Corruption Commissioner; or (b) a Deputy Commissioner (within the meaning of the *National Anti-Corruption Commission Act 2022*); or (c) a National Anti-Corruption Commission officer authorised under section 6B	(a) the National Anti-Corruption Commissioner; or (b) a Deputy Commissioner (within the meaning of the *National Anti-Corruption Commission Act 2022*); or (c) a National Anti-Corruption Commission officer who is an SES employee the chief officer authorises under subsection (5)
15	Australian Crime Commission	the Chief Executive Officer of the Commission	(a) the Chief Executive Officer; or (b) a person covered by a paragraph of the definition of ***member of the***	(a) the Chief Executive Officer; or (b) an executive level member of the staff of the ACC the chief officer

Authorised Version C2025C00651 registered 28/11/2025

Federal law enforcement agencies				
	Column 1	**Column 2**	**Column 3**	**Column 4**
	Law enforcement agency	**Chief officer**	**Law enforcement officer**	**Appropriate authorising officer**
			staff of the ACC in section 4 of the *Australian Crime Commission Act 2002*	authorises under subsection (5)

(7) This table deals with State and Territory law enforcement agencies:

State and Territory law enforcement agencies				
	Column 1	**Column 2**	**Column 3**	**Column 4**
	Law enforcement agency	**Chief officer**	**Law enforcement officer**	**Appropriate authorising officer**
5	police force of a State or Territory	the Commissioner of Police in the police force, or the person holding equivalent rank	(a) an officer (however described) of the police force; or (b) a person seconded to the police force	(a) the Commissioner or the person holding equivalent rank; or (b) an Assistant Commissioner or a person holding equivalent rank; or (c) a Superintendent or a person holding equivalent rank
10	Independent Commission Against	the Chief Commissioner of the	an officer of the Commission (within the meaning	(a) the Chief Commissioner; or

Authorised Version C2025C00651 registered 28/11/2025

State and Territory law enforcement agencies				
	Column 1	**Column 2**	**Column 3**	**Column 4**
	Law enforcement agency	**Chief officer**	**Law enforcement officer**	**Appropriate authorising officer**
	Corruption of New South Wales	Commission	of the *Independent Commission Against Corruption Act 1988* (NSW))	(b) a Commissioner; or (c) an Assistant Commissioner; or (d) an executive level officer of the Commission whom the chief officer authorises under subsection (5)
15	New South Wales Crime Commission	the Commissioner for the Commission	(a) a member of the Commission; or (b) a member of the staff of the Commission; (within the meaning of the *New South Wales Crime Commission Act 1985* (NSW))	(a) a member of the Commission; or (b) an executive level member of the Staff of the Commission the chief officer authorises under subsection (5)
20	Law Enforcement Conduct Commission of New South Wales	the Chief Commissioner of the Commission	an officer of the Commission (within the meaning of the Law Enforcement Conduct Commission Act 2016 (NSW))	(a) the Chief Commissioner; or (b) the Commissioner for Integrity; or (c) an Assistant Commissioner, or an executive level member of

Authorised Version C2025C00651 registered 28/11/2025

State and Territory law enforcement agencies				
	Column 1	**Column 2**	**Column 3**	**Column 4**
	Law enforcement agency	**Chief officer**	**Law enforcement officer**	**Appropriate authorising officer**
				staff of the Commission (within the meaning of that Act), the chief officer authorises under subsection (5)
22	Independent Broad-based Anti-corruption Commission of Victoria	the Commissioner of the Commission	an IBAC Officer (within the meaning of the *Independent Broad-based Anti-corruption Commission Act 2011* (Vic.))	(a) the Commissioner; or (b) a Deputy Commissioner of the Commission; or (c) the Chief Executive Officer of the Commission; or (d) an executive level sworn IBAC Officer (within the meaning of that Act) the chief officer authorises under subsection (5)
25	Crime and Corruption Commission of Queensland	the chairman of the Commission	an authorised commission officer (within the meaning of the *Crime and Corruption Act 2001* (Qld))	(a) the chairman; or (b) a senior executive officer (within the meaning of that Act)

Authorised Version C2025C00651 registered 28/11/2025

State and Territory law enforcement agencies				
	Column 1	**Column 2**	**Column 3**	**Column 4**
	Law enforcement agency	**Chief officer**	**Law enforcement officer**	**Appropriate authorising officer**
30	Corruption and Crime Commission of Western Australia	the Commissioner of the Commission	an officer of the Commission (within the meaning of the *Corruption and Crime Commission Act 2003* (WA))	the Commissioner
35	Independent Commission Against Corruption of South Australia	the Commissioner of the Commission	(a) the Commissioner; or (b) the Deputy Commissioner; or (c) a member of the staff of the Commission; or (d) an examiner or investigator (within the meaning of the *Independent Commission Against Corruption Act 2012* (SA)) of the Commission	(a) the Commissioner; or (b) the Deputy Commissioner; or (c) an executive level member of the staff of the Commission the chief officer authorises under subsection (5)

(8) A person is ***executive level***, in relation to a law enforcement agency of a State, if the person occupies an office or position at an equivalent level to that of:

(a) if the State is New South Wales—a Public Service senior executive (within the meaning of the *Government Sector Employment Act 2013* (NSW)); or

Authorised Version C2025C00651 registered 28/11/2025

(aa) if the State is Victoria—an executive (within the meaning of the *Public Administration Act 2004* (Vic.)); or

(b) if the State is South Australia—an executive employee (within the meaning of the *Public Sector Act 2009* (SA)).

6B Authorisation of law enforcement officer

The National Anti-Corruption Commissioner may authorise, in writing, a National Anti-Corruption Commission officer to be a law enforcement officer of the National Anti-Corruption Commission.

6C When a Part 5.3 supervisory order is taken to be in force

For the purposes of this Act, a Part 5.3 supervisory order is taken to be in force in relation to a person if:

(a) the order is a control order that has been made but has not yet come into force because:

(i) it has not been served on the person; or

(ii) the person is detained in custody in a prison; or

(b) the order is an extended supervision order or an interim supervision order that has been made but the period specified in the order under paragraph 105A.7A(4)(d) or 105A.9A(7)(c) of the *Criminal Code* has not yet begun.

6D Succeeding Part 5.3 supervisory orders

(1) If 2 or more successive control orders are made in relation to the same person, each later control order is a ***succeeding Part 5.3 supervisory order*** in relation to each earlier control order.

Note: If an interim control order is confirmed, the confirmed control order is a succeeding Part 5.3 supervisory order in relation to the interim control order (see the definition of ***control order*** in section 6).

(2) If an interim supervision order is made in relation to a person, any later extended supervision order in relation to the person is a ***succeeding Part 5.3 supervisory order*** in relation to an earlier interim supervision order.

Authorised Version C2025C00651 registered 28/11/2025

(3) If 2 or more successive extended supervision orders or interim supervision orders are made in relation to the same person, each later extended supervision order or interim supervision order is a ***succeeding Part 5.3 supervisory order*** in relation to each earlier extended supervision order or interim supervision order.

6E When a community safety supervision order is taken to be in force

For the purposes of this Act, a community safety supervision order is taken to be in force in relation to a person if the order has been made but the period specified in the order under paragraph 395.13(5)(d) of the *Criminal Code* has not yet begun.

6F Succeeding community safety supervision order

(1) If a community safety supervision order is made in relation to a person, any later community safety supervision order in relation to the person is a ***succeeding community safety supervision order*** in relation to an earlier community safety supervision order.

(2) If 2 or more successive community safety supervision orders are made in relation to the same person, each later community safety supervision order is a ***succeeding community safety supervision order*** in relation to each earlier community safety supervision order.

7 State offence that has a federal aspect

An offence against a law of a State is taken, for the purposes of this Act, to be a State offence that has a federal aspect:

(a) in a case where the offence is being investigated by the Australian Federal Police—if it would be taken to be a State offence that has a federal aspect under section 4AA of the *Australian Federal Police Act 1979*; and

(b) in a case where the offence is being investigated by the Australian Crime Commission—if it would be taken to be a

Authorised Version C2025C00651 registered 28/11/2025

State offence that has a federal aspect under section 4A of the *Australian Crime Commission Act 2002*; and

(c) in any other case—if it would be taken to be a State offence that has a federal aspect if either of the sections referred to in paragraphs (a) and (b) were to apply.

7A Criminal network of individuals

(1) For the purposes of this Act, a ***criminal network of individuals*** is an electronically linked group of individuals, where:

(a) in a case where each individual in the group uses, or is likely to use, the same electronic service as at least one other individual in the group—the use of that electronic service enables any of the individuals in the group to:

(i) engage in conduct that constitutes a relevant offence; or

(ii) communicate with any of the individuals in the group about any of the individuals in the group engaging in conduct that constitutes a relevant offence; or

(iii) facilitate the engagement, by another person (whether or not an individual in the group), in conduct that constitutes a relevant offence; or

(iv) communicate with any of the individuals in the group about facilitating the engagement, by another person (whether or not an individual in the group), in conduct that constitutes a relevant offence; or

(b) in a case where each individual in the group communicates with at least one other individual in the group by electronic communication—the electronic communication enables any of the individuals in the group to:

(i) engage in conduct that constitutes a relevant offence; or

(ii) communicate with any of the individuals in the group about any of the individuals in the group engaging in conduct that constitutes a relevant offence; or

(iii) facilitate the engagement, by another person (whether or not an individual in the group), in conduct that constitutes a relevant offence; or

Authorised Version C2025C00651 registered 28/11/2025

(iv) communicate with any of the individuals in the group about facilitating the engagement, by another person (whether or not an individual in the group), in conduct that constitutes a relevant offence.

(2) For the purposes of subsection (1), it is immaterial whether:

(a) the identities of the individuals in the group can be ascertained; or

(b) the details of the relevant offences can be ascertained; or

(c) there are likely to be changes, from time to time, in the composition of the group.

8 External Territories

This Act extends to every external Territory.

9 Binding the Crown

(1) This Act binds the Crown in each of its capacities.

(2) This Act does not make the Crown liable to be prosecuted for an offence.

Authorised Version C2025C00651 registered 28/11/2025

Part 2—Warrants

Division 1—Introduction

10 Types of warrant

(1) The following types of warrant may be issued under this Part:
  (a) a surveillance device warrant;
  (b) a retrieval warrant;
  (c) a computer access warrant;
  (d) a data disruption warrant;
  (e) a network activity warrant.

(2) A surveillance device warrant or a retrieval warrant may be issued:
  (a) in respect of more than one kind of surveillance device; and
  (b) in respect of more than one surveillance device of any particular kind.

11 Who may issue etc. warrants?

(1) Any warrant under this Part may be issued by:
  (a) in relation to an application for a warrant by a law enforcement officer of the National Anti-Corruption Commission—an eligible Judge; or
  (b) otherwise—an eligible Judge or a nominated ART member.

Warrants issued to law enforcement officers of the NACC

(2) An application made under this Part by a law enforcement officer of the National Anti-Corruption Commission may be made only to an eligible Judge.

Note: An application under this Part may be for a warrant, or to extend or vary a warrant.

Authorised Version C2025C00651 registered 28/11/2025

(3) A warrant issued under this Part to a law enforcement officer of the National Anti-Corruption Commission may be revoked only by an eligible Judge.

Note: Warrants may be revoked under this Part by an eligible Judge or nominated ART member on their own initiative. As a result of this subsection, warrants issued to law enforcement officers of the National Anti-Corruption Commission may be revoked only by an eligible Judge.

12 Eligible Judges

(1) In this section, unless the contrary intention appears:

eligible Judge means a person:

(a) in relation to whom a consent under subsection (2) and a declaration under subsection (3) are in force; and

(b) in relation to any of the following issued to, or applied for by, a law enforcement officer of the National Anti-Corruption Commission—who is a superior Court Judge:

(i) a warrant;

(ii) an emergency authorisation;

(iii) an assistance order (within the meaning of subsection 64A(1)).

Judge means a person who is a Judge of a court created by the Parliament.

(2) A Judge may, by writing, consent to be declared an eligible Judge under subsection (3) by the Minister referred to in that subsection.

(3) The Minister administering the *Judiciary Act 1903* may, by writing, declare Judges in relation to whom consents are in force under subsection (2) to be eligible Judges for the purposes of this Act.

(4) Any function or power conferred on the Judge under this Act is so conferred only in a personal capacity and not as a court or a member of a court.

Authorised Version C2025C00651 registered 28/11/2025

(5) An eligible Judge has, in relation to the performance or exercise of a function or power conferred on an eligible Judge by this Act, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

(6) An instrument declaring a Judge to be an eligible Judge is not a legislative instrument.

13 Nominated ART members

(1) The Minister administering the *Administrative Review Tribunal Act 2024* (the ***ART Minister***) may, by writing, nominate a person who holds one of the following appointments to the Administrative Review Tribunal to issue warrants (except to law enforcement officers of the National Anti-Corruption Commission) under this Part:
  (a) Deputy President;
  (b) a senior member;
  (c) a general member.

(2) Despite subsection (1), the ART Minister must not nominate a person who holds an appointment as a senior member on a sessional basis, or as a general member, of the Tribunal unless the person:
  (a) is enrolled as a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or of the Australian Capital Territory; and
  (b) has been so enrolled for not less than 5 years.

(3) A nomination ceases to have effect if:
  (a) the nominated ART member ceases to hold an appointment described in subsection (1); or
  (b) the ART Minister, by writing, withdraws the nomination.

(4) A nominated ART member has, in relation to the performance or exercise of a function or power conferred on a nominated ART member by this Act, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

Authorised Version C2025C00651 registered 28/11/2025

Division 2—Surveillance device warrants

14 Application for surveillance device warrant

Warrants sought for offence investigations

(1) A law enforcement officer (or another person on his or her behalf) may apply for the issue of a surveillance device warrant if the law enforcement officer suspects on reasonable grounds that:

(a) one or more relevant offences have been, are being, are about to be, or are likely to be, committed; and

(b) an investigation into those offences is being, will be, or is likely to be, conducted; and

(c) the use of a surveillance device is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of the commission of the relevant offences or the identity or location of the offenders.

(2) If the application is being made by or on behalf of a State or Territory law enforcement officer, the reference in subsection (1) to a relevant offence does not include a reference to a State offence that has a federal aspect.

Warrants sought for recovery orders

(3) A law enforcement officer (or another person on his or her behalf) may apply for the issue of a surveillance device warrant if:

(a) a recovery order is in force; and

(b) the law enforcement officer suspects on reasonable grounds that the use of a surveillance device may assist in the location and safe recovery of the child to whom the recovery order relates.

Warrants sought for international assistance investigations

(3A) A law enforcement officer (or a person on his or her behalf) may apply for the issue of a surveillance device warrant if he or she:

Authorised Version C2025C00651 registered 28/11/2025

(a) is authorised to do so under an international assistance authorisation; and

(b) suspects on reasonable grounds that the use of a surveillance device is necessary, in the course of the investigation, proceeding or investigative proceeding to which the authorisation relates, for the purpose of enabling evidence to be obtained of:

(i) the commission of an offence to which the authorisation relates; or

(ii) the identity or location of the persons suspected of committing the offence.

Warrants sought for integrity operations

(3B) A federal law enforcement officer (or another person on his or her behalf) may apply for the issue of a surveillance device warrant if:

(a) an integrity authority is in effect authorising an integrity operation in relation to an offence that it is suspected has been, is being or is likely to be committed by a staff member of a target agency; and

(b) the federal law enforcement officer suspects on reasonable grounds that the use of a surveillance device will assist the conduct of the integrity operation by:

(i) recording or monitoring the operation; and

(ii) enabling evidence to be obtained relating to the commission of the offence or the integrity, location or identity of any staff member of the target agency.

Warrants sought for post-sentence order applications

(3BA) A law enforcement officer (or another person on the officer's behalf) may apply for the issue of a surveillance device warrant if:

(a) a person is a terrorist offender in relation to whom an application for a post-sentence order could be made; and

(b) the person is detained in custody in a prison; and

Authorised Version C2025C00651 registered 28/11/2025

(c) the officer suspects on reasonable grounds that there is an appreciable risk of the person committing a serious Part 5.3 or 5.3A offence; and

(d) consideration is being given, will be given, or is likely to be given, by the AFP Minister (or a person on behalf of the AFP Minister), as to whether to apply for a post-sentence order in relation to the person; and

(e) the officer suspects on reasonable grounds that the use of a surveillance device to obtain information would be likely to assist in determining whether to apply for the post-sentence order.

Warrants sought for Part 5.3 supervisory orders

(3C) A law enforcement officer (or another person on his or her behalf) may apply for the issue of a surveillance device warrant if:

(a) a Part 5.3 supervisory order is in force in relation to a person; and

(b) the law enforcement officer suspects on reasonable grounds that the use of a surveillance device to obtain information relating to the person would be likely to substantially assist in:

(i) achieving a Part 5.3 object; or

(ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with.

Note: For Part 5.3 supervisory orders that have been made but not come into force, see section 6C.

Warrants sought for Part 9.10 order applications

(3D) A law enforcement officer (or another person on the officer's behalf) may apply for the issue of a surveillance device warrant if:

(a) a person is a serious offender in relation to whom an application for a Part 9.10 order could be made; and

Authorised Version C2025C00651 registered 28/11/2025

(b) the officer suspects on reasonable grounds that there is an appreciable risk of the person committing a serious violent or sexual offence; and

(c) consideration is being given, will be given, or is likely to be given, by the Immigration Minister (or a person on behalf of the Immigration Minister), as to whether to apply for a Part 9.10 order in relation to the person; and

(d) the officer suspects on reasonable grounds that the use of a surveillance device to obtain information would be likely to assist in determining whether to apply for the Part 9.10 order.

Warrants sought for community safety supervision orders

(3E) A law enforcement officer (or another person on the officer's behalf) may apply for the issue of a surveillance device warrant if:

(a) a community safety supervision order is in force in relation to a person; and

(b) the law enforcement officer suspects on reasonable grounds that the use of a surveillance device to obtain information relating to the person would be likely to substantially assist in:

(i) achieving a Part 9.10 object; or

(ii) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with.

Note: For community safety supervision orders that have been made but not come into force, see section 6E.

Procedure for making applications

(4) The application under subsection (1), (3), (3A), (3B), (3BA), (3C), (3D) or (3E) may be made to an eligible Judge or to a nominated ART member.

(5) An application:

(a) must specify:

(i) the name of the applicant; and

Authorised Version C2025C00651 registered 28/11/2025

(ii) the nature and duration of the warrant sought, including the kind of surveillance device or devices 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.

(6) If a law enforcement officer believes that:

(a) the immediate use of a surveillance device is necessary for a purpose referred to in paragraph (1)(c) or may assist as described in paragraph (3)(b), or would be likely to substantially assist as described in paragraph (3C)(b) or (3E)(b); and

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

an application for a warrant may be made before an affidavit is prepared or sworn.

(7) If subsection (6) applies, the applicant must:

(a) provide as much information as the eligible Judge or nominated ART member considers is reasonably practicable in the circumstances; and

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

15 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 14 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 transmit a copy of the affidavit, whether sworn or unsworn, to the eligible Judge or to the nominated ART member who is to determine the application.

Authorised Version C2025C00651 registered 28/11/2025

16 Determining the application

(1) An eligible Judge or a nominated ART member may issue a surveillance device warrant if satisfied:

(a) in the case of a warrant sought in relation to a relevant offence—that there are reasonable grounds for the suspicion founding the application for the warrant; and

(b) in the case of a warrant sought in relation to a recovery order—that such an order is in force and that there are reasonable grounds for the suspicion founding the application for the warrant; and

(ba) in the case of a warrant sought in relation to an international assistance authorisation—that such an authorisation is in force and that there are reasonable grounds for the suspicion founding the application for the warrant; and

(bb) in the case of a warrant sought for the purposes of an integrity operation—that the integrity authority for the operation is in effect, and that there are reasonable grounds for the suspicions founding the application for the warrant (as mentioned in paragraphs 14(3B)(a) and (b)); and

(bba) in the case of a warrant sought to determine whether to apply for a post-sentence order—that the conditions in paragraphs 14(3BA)(a), (b) and (d) are met, and that there are reasonable grounds for the suspicions founding the application for the warrant (as mentioned in paragraphs 14(3BA)(c) and (e)); and

(bc) in the case of a warrant sought in relation to a Part 5.3 supervisory order that is in force in relation to a person—that the order is in force in relation to the person, and that there are reasonable grounds for the suspicion founding the application for the warrant (as mentioned in paragraph 14(3C)(b)); and

(bd) in the case of a warrant sought to determine whether to apply for a Part 9.10 order—that the conditions in paragraphs 14(3D)(a) and (c) are met, and that there are reasonable grounds for the suspicions founding the application for the warrant (as mentioned in paragraphs 14(3D)(b) and (d)); and

Authorised Version C2025C00651 registered 28/11/2025

(be) in the case of a warrant sought in relation to a community safety supervision order that is in force in relation to a person—that the order is in force in relation to the person, and that there are reasonable grounds for the suspicion founding the application for the warrant (as mentioned in paragraph 14(3E)(b)); and

(c) in the case of an unsworn application—that it would have been impracticable for an affidavit to have been sworn or prepared before the application was made; and

(d) in the case of a remote application—that it would have been impracticable for the application to have been made in person.

Note: For Part 5.3 supervisory orders that have been made but not come into force, see section 6C. For community safety supervision orders that have been made but not come into force, see section 6E.

(2) In determining whether a surveillance device warrant should be issued, the eligible Judge or nominated ART member must have regard to:

(a) in the case of a warrant sought in relation to a relevant offence or an international assistance authorisation, or for the purposes of an integrity operation—the nature and gravity of the alleged offence; and

(b) in the case of a warrant sought to assist in the location and safe recovery of a child to whom a recovery order relates—the circumstances that gave rise to the making of the order; and

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

(d) the existence of any alternative means of obtaining the evidence or information sought to be obtained; and

(e) in the case of a warrant sought in relation to a relevant offence or a recovery order, or for the purposes of an integrity operation—the likely evidentiary or intelligence value of any evidence or information sought to be obtained; and

Authorised Version C2025C00651 registered 28/11/2025

(ea) in the case of a warrant sought in relation to an international assistance authorisation—the likely evidentiary or intelligence value of any evidence or information sought to be obtained, to the extent that this is possible to determine from information obtained from the international entity to which the authorisation relates; and

(f) in the case of a warrant sought in relation to a relevant offence or a recovery order—any previous warrant sought or issued under this Division in connection with the same alleged offence or the same recovery order.

(3) In addition to the matters in subsection (2), in determining whether to issue a surveillance device warrant sought to determine whether to apply for a post-sentence order in relation to a person, the eligible Judge or nominated ART member must have regard to:

(a) the likely value of the information sought to be obtained in determining whether to apply for the post-sentence order; and

(b) any previous application for a surveillance device warrant sought or issued to determine whether to apply for a post-sentence order in relation to the person.

(3A) In addition to the matters in subsection (2), in determining whether to issue a surveillance device warrant sought to determine whether to apply for a Part 9.10 order in relation to a person, the eligible Judge or nominated ART member must have regard to:

(a) the likely value of the information sought to be obtained in determining whether to apply for the Part 9.10 order; and

(b) any previous application for a surveillance device warrant sought or issued to determine whether to apply for a Part 9.10 order in relation to the person.

(4) In addition to the matters in subsection (2), in determining whether to issue a surveillance device warrant sought in a case where a Part 5.3 supervisory order is in force in relation to a person, the eligible Judge or nominated ART member must have regard to:

(a) the likely value of the information sought to be obtained, in:

(i) achieving a Part 5.3 object; or

Authorised Version C2025C00651 registered 28/11/2025

(ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and

(b) whether the use of the surveillance device in accordance with the warrant would be the means of obtaining the evidence or information sought to be obtained, that is likely to have the least interference with any person's privacy; and

(c) if the order is a control order:

(i) the possibility that the person has engaged, is engaging, or will engage, in a terrorist act; or

(ii) the possibility that the person has provided, is providing, or will provide, support for a terrorist act; or

(iii) the possibility that the person has facilitated, is facilitating, or will facilitate, a terrorist act; or

(iv) the possibility that the person has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country; or

(v) the possibility that the person has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country; and

(d) if the order is an extended supervision order or interim supervision order—the possibility that the person has committed, is committing, or will commit, a serious Part 5.3 or 5.3A offence; and

(e) in relation to any Part 5.3 supervisory order—the possibility that the person has contravened, is contravening, or will contravene, the order or a succeeding Part 5.3 supervisory order; and

(f) any previous surveillance device warrant sought or issued on the basis of a Part 5.3 supervisory order that is or was in force in relation to the person.

(5) In addition to the matters in subsection (2), in determining whether to issue a surveillance device warrant sought in a case where a community safety supervision order is in force in relation to a person, the eligible Judge or nominated ART member must have regard to:

Authorised Version C2025C00651 registered 28/11/2025

(a) the likely value of the information sought to be obtained, in:
  (i) achieving a Part 9.10 object; or
  (ii) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with; and
(b) whether the use of the surveillance device in accordance with the warrant would be the means of obtaining the evidence or information sought to be obtained, that is likely to have the least interference with any person's privacy; and
(c) the possibility that the person has committed, is committing, or will commit, a serious violent or sexual offence; and
(d) the possibility that the person has contravened, is contravening, or will contravene, the community safety supervision order or a succeeding community safety supervision order; and
(e) any previous surveillance device warrant sought or issued on the basis of a community safety supervision order that is or was in force in relation to the person.

17 What must a surveillance device warrant contain?

(1) A surveillance device warrant must:
  (a) state that the eligible Judge or nominated ART member issuing the warrant is satisfied of the matters referred to in subsection 16(1) and has had regard to the matters referred to in subsections 16(2), (3), (3A), (4) and (5) (as the case requires); and
  (b) specify:
    (i) the name of the applicant; and
    (ii) if the warrant relates to one or more alleged relevant offences—the alleged offences in respect of which the warrant is issued; and
    (iii) if the warrant relates to a recovery order—the date the order was made and the name of the child to whom the order relates; and

Authorised Version C2025C00651 registered 28/11/2025

(iiia) if the warrant relates to an international assistance authorisation—each offence to which the authorisation relates; and

(iiib) if the warrant is issued for the purposes of an integrity operation—the integrity authority for the operation and each alleged relevant offence in relation to which the authority was granted; and

(iv) the date the warrant is issued; and

(v) the surveillance device or devices authorised to be used; and

(vi) if the warrant authorises the use of a surveillance device on premises—the premises on which the use of the surveillance device is authorised; and

(vii) 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; and

(viii) if the warrant authorises the use of a surveillance device in respect of the conversations, activities or location of a person—the name of the person (if known) or the fact that the person's identity is unknown; and

(ix) the period during which the warrant is in force (see subsection (1A)); and

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

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

(1AA) If a surveillance device warrant is issued to determine whether to apply for a post-sentence order in relation to a person, the warrant must also specify the name of the person.

(1AB) If a warrant is issued on the basis of a Part 5.3 supervisory order that is in force in relation to a person, the warrant must also specify the following details in relation to the order:

(a) the name of the person;

Authorised Version C2025C00651 registered 28/11/2025

(b) the date the order was made;

(c) if (disregarding section 6C) the order is not already in force and the order is not an interim control order—when the order comes into force;

(d) whether the order is:

(i) an interim control order; or

(ii) a confirmed control order; or

(iii) an interim supervision order; or

(iv) an extended supervision order.

(1AC) If a surveillance device warrant is issued to determine whether to apply for a Part 9.10 order in relation to a person, the warrant must also specify the name of the person.

(1AD) If a warrant is issued on the basis of a community safety supervision order that is in force in relation to a person, the warrant must also specify the following details in relation to the order:

(a) the name of the person;

(b) the date the order was made;

(c) if (disregarding section 6E) the order is not already in force—when the order comes into force.

(1A) A warrant may only be issued:

(a) for a period of no more than 90 days; or

(b) if the warrant is issued for the purposes of an integrity operation—for a period of no more than 21 days.

Note: The use of a surveillance device pursuant to a warrant may be discontinued earlier: see section 21.

(1B) To avoid doubt, a warrant issued on the basis that a Part 5.3 supervisory order is in force remains in force for the period mentioned in paragraph (1A)(a) even if the order ceases to be in force, provided that the order is replaced by a succeeding Part 5.3 supervisory order.

Note 1: If there is no succeeding Part 5.3 supervisory order, the warrant must be revoked (see section 21).

Authorised Version C2025C00651 registered 28/11/2025

Note 2: A control order is not a succeeding Part 5.3 supervisory order in relation to an extended supervision order, and vice versa (see section 6D).

(1C) To avoid doubt, a warrant issued on the basis that a community safety supervision order is in force remains in force for the period mentioned in paragraph (1A)(a) even if the order ceases to be in force, provided that the order is replaced by a succeeding community safety supervision order.

Note: If there is no succeeding community safety supervision order, the warrant must be revoked (see section 21).

(2) In the case of a warrant authorising the use of a surveillance device on premises that are vehicles, the warrant need only specify the class of vehicle in relation to which the use of the surveillance device is authorised.

(3) A warrant must be signed by the person issuing it and include his or her name.

(4) As soon as practicable after completing and signing a warrant issued on a remote application, the person issuing it must:

(a) inform the applicant of:

(i) the terms of the warrant; and

(ii) the date on which and the time at which the warrant was issued; and

(b) give the warrant to the applicant while retaining a copy of the warrant for the person's own record.

18 What a surveillance device warrant authorises

(1) A surveillance device warrant (subject to any conditions specified in it) may authorise one or more of the following:

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

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

(c) the use of a surveillance device in respect of the conversations, activities or location of a specified person or a person whose identity is unknown.

Authorised Version C2025C00651 registered 28/11/2025

(2) A surveillance device warrant authorises:

(a) for a warrant of a kind referred to in paragraph (1)(a):

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

(ii) the entry, by force if necessary, onto the premises, and onto other specified premises adjoining or providing access to the premises, for any of the purposes referred to in subparagraph (i) or subsection (3); and

(b) for a warrant of a kind referred to in paragraph (1)(b):

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

(ii) the entry, by force if necessary, onto any premises where the object, or an object of the class, is reasonably believed to be or is likely to be, and onto other premises adjoining or providing access to those premises, for any of the purposes referred to in subparagraph (i) or subsection (3); and

(c) for a warrant of a kind referred to in paragraph (1)(c):

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

(ii) the entry, by force if necessary, onto the premises, or other premises adjoining or providing access to those premises, for any of the purposes referred to in subparagraph (i) or subsection (3).

(3) Each surveillance device warrant also authorises:

(a) the retrieval of the surveillance device; and

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

(c) the temporary removal of an object or vehicle from premises for the installation, maintenance or retrieval of the

Authorised Version C2025C00651 registered 28/11/2025

surveillance device or enhancement equipment and the return of the object or vehicle to the premises; and

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

(e) the connection of the surveillance device or enhancement equipment to any source of electricity and the use of electricity from that source to operate the device or equipment; and

(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 device or equipment; and

(g) the provision of assistance or technical expertise to the law enforcement officer primarily responsible for the execution of 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 surveillance device warrant may authorise the interference with property of a person who is not the subject of the investigation in respect of which the warrant was issued but, if the interference would be on premises not specified in the warrant, only if the person issuing the warrant is satisfied that it is necessary to do so in order to give effect to the warrant.

(6) A law enforcement officer may use a surveillance device under a warrant only in the performance of his or her duty.

(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*.

Authorised Version C2025C00651 registered 28/11/2025

19 Extension and variation of surveillance device warrant

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

(a) for an extension of the warrant for a period of no more than:

(i) 90 days after the day the warrant would otherwise expire; or

(ii) if the warrant is issued for the purposes of an integrity operation—21 days after the day the warrant would otherwise expire; or

(b) for a variation of any of the other terms of the warrant.

(2) The application is to be made to an eligible Judge or to a nominated ART member and must be accompanied by the original warrant.

(3) Sections 14 and 15 apply, with any necessary changes, to an application under this section as if it were an application for the warrant.

(4) The Judge or member may grant an application if satisfied that the matters referred to in subsection 16(1) still exist, having regard to the matters in subsections 16(2), (3), (3A), (4) and (5) (as the case requires).

(5) If the Judge or member grants the application, the Judge or member must endorse the new expiry date or the other varied term on the original warrant.

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

20 Revocation of surveillance device warrant

(1) A surveillance device warrant may, by instrument in writing, be revoked by an eligible Judge or nominated ART member on his or her own initiative at any time before the expiration of the period of validity specified in the warrant.

Authorised Version C2025C00651 registered 28/11/2025

(2) If the circumstances set out in subsection 21(2), (3) or (3A) apply in relation to a surveillance device warrant, the chief officer of the law enforcement agency to which the law enforcement officer to whom the warrant was issued belongs or is seconded must, by instrument in writing, revoke the warrant.

(3) The instrument revoking a warrant must be signed by the eligible Judge, the nominated ART member or the chief officer of the law enforcement agency, as the case requires.

(4) If an eligible Judge or nominated ART member revokes a warrant, he or she must give a copy of the instrument of revocation to the chief officer of the law enforcement agency to which the law enforcement officer to whom the warrant was issued belongs or is seconded.

(5) If:

(a) an eligible Judge or nominated ART member revokes a warrant; and

(b) at the time of the revocation, a law enforcement officer is executing the warrant;

the law enforcement officer is not subject to any civil or criminal liability for any act done in the proper execution of that warrant before the officer is made aware of the revocation.

21 Discontinuance of use of surveillance device under warrant

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

Obligations on chief officers

(2) If:

(a) the surveillance device warrant has been sought by or on behalf of a law enforcement officer; and

(b) the chief officer of the law enforcement agency to which the law enforcement officer belongs or is seconded is satisfied that:

Authorised Version C2025C00651 registered 28/11/2025

(i) the use of a surveillance device under the warrant is no longer required for the purpose for which it was sought; or

(ii) without limiting subparagraph (i), if the warrant was sought for the purposes of an integrity operation—the integrity authority for the integrity operation is no longer in effect; and

(c) the warrant was not issued to determine whether to apply for a post-sentence order; and

(d) the warrant was not issued to determine whether to apply for a Part 9.10 order;

the chief officer must (subject to subsections (3) and (3A)), in addition to revoking the warrant under section 20, take the steps necessary to ensure that use of the surveillance device authorised by the warrant is discontinued.

(3) The chief officer is required to take steps under subsection (2) in relation to a surveillance device warrant that is issued on the basis of a Part 5.3 supervisory order that was in force in relation to a person only if neither the Part 5.3 supervisory order, nor any succeeding Part 5.3 supervisory order, is in force in relation to the person.

Note: A control order is not a succeeding Part 5.3 supervisory order in relation to an extended supervision order, and vice versa (see section 6D).

(3A) The chief officer is required to take steps under subsection (2) in relation to a surveillance device warrant that is issued on the basis of a community safety supervision order that was in force in relation to a person only if neither the community safety supervision order, nor any succeeding community safety supervision order, is in force in relation to the person.

(4) If the chief officer of a law enforcement agency is notified that a warrant has been revoked by an eligible Judge or a nominated ART member under section 20, the chief officer must take the steps necessary to ensure that use of the surveillance device authorised by the warrant is discontinued as soon as practicable.

Authorised Version C2025C00651 registered 28/11/2025

Obligations on law enforcement officers to whom warrants are issued etc.

(5) If the law enforcement officer to whom the warrant is issued, or who is primarily responsible for executing the warrant, believes that:

(a) use of a surveillance device under the warrant is no longer required for the purpose for which the warrant was issued; or

(b) without limiting paragraph (a), if the warrant was sought for the purposes of an integrity operation—the integrity authority for the integrity operation is no longer in effect;

the officer must (subject to subsections (6) and (7)) immediately inform the chief officer of the law enforcement agency to which the officer belongs or is seconded.

(6) If the law enforcement officer to whom a warrant is issued, or who is primarily responsible for executing a warrant issued, on the basis that a Part 5.3 supervisory order was in force in relation to a person believes that neither that order, nor any succeeding Part 5.3 supervisory order, is in force in relation to the person, the officer must immediately inform the chief officer of the law enforcement agency to which the officer belongs or is seconded.

(7) If the law enforcement officer to whom a warrant is issued, or who is primarily responsible for executing a warrant issued, on the basis that a community safety supervision order was in force in relation to a person believes that neither that order, nor any succeeding community safety supervision order, is in force in relation to the person, the officer must immediately inform the chief officer of the law enforcement agency to which the officer belongs or is seconded.

Authorised Version C2025C00651 registered 28/11/2025

Division 3—Retrieval warrants

22 Application for retrieval warrant

(1) A law enforcement officer (or another person on his or her behalf) may apply for the issue of a retrieval warrant in respect of a surveillance device that:

(a) was lawfully installed on premises, or in or on an object, under:

(i) a surveillance device warrant; or

(ii) a tracking device authorisation; and

(b) the law enforcement officer suspects 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 an eligible Judge or to a nominated ART member.

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

(4) 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 the application for a retrieval warrant is made;

the application may be made before an affidavit is prepared or sworn.

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

(a) provide as much information as the eligible Judge or nominated ART member considers is reasonably practicable in the circumstances; and

(b) not later than 72 hours following the making of the application, send a duly sworn affidavit to the eligible Judge

Authorised Version C2025C00651 registered 28/11/2025

or nominated ART member who determined the application, whether or not a warrant has been issued.

23 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 22 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 transmit a copy of the affidavit, whether sworn or unsworn, to the eligible Judge or nominated ART member who is to determine the application.

24 Determining the application

(1) An eligible Judge or nominated ART member may issue a retrieval warrant if the Judge or member is satisfied:
  (a) that there are reasonable grounds for the suspicion founding the application for the warrant; and
  (b) in the case of an unsworn application—that it would have been impracticable for an affidavit to have been sworn or prepared before the application was made; and
  (c) in the case of a remote application—that it would have been impracticable for the application to have been made in person.

(2) In determining whether a retrieval warrant should be issued, the eligible Judge or nominated ART member 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.

Authorised Version C2025C00651 registered 28/11/2025

25 What must a retrieval warrant contain?

(1) A retrieval warrant must:

(a) state that the eligible Judge or nominated ART member is satisfied of the matters referred to in subsection 24(1) and has had regard to the matters referred to in subsection 24(2); and

(b) specify:

(i) the name of the applicant; and

(ii) the date the warrant is issued; and

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

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

(v) the period (not exceeding 90 days) during which the warrant is in force; and

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

(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 his or her name.

(3) As soon as practicable after completing and signing a warrant issued on a remote application, the person issuing it must:

(a) inform the applicant of:

(i) the terms of the warrant; and

(ii) the date on which and the time at which the warrant was issued; and

(b) give the warrant to the applicant while retaining a copy of the warrant for the person's own record.

26 What a retrieval warrant authorises

(1) A retrieval warrant (subject to any conditions specified in it) authorises:

Authorised Version C2025C00651 registered 28/11/2025

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

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

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

(d) if the device or equipment is installed on or in an object or vehicle—the temporary removal of the object or vehicle from any place where it is situated for the purpose of retrieving the device and equipment and returning the object or vehicle to that place; and

(e) the provision of assistance or technical expertise to the law enforcement officer named in 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 but cannot authorise the use, for any purpose, of the surveillance device specified in the warrant.

27 Revocation of retrieval warrant

(1) A retrieval warrant may, by instrument in writing, be revoked by an eligible Judge or a nominated ART member on his or her own initiative at any time before the expiration of the period of validity specified in the warrant.

Authorised Version C2025C00651 registered 28/11/2025

(2) If the chief officer of the law enforcement agency to which the law enforcement officer to whom a retrieval warrant was issued belongs or is seconded is satisfied that the grounds for issue of the retrieval warrant no longer exist—the chief officer must, by instrument in writing, revoke the warrant.

(3) The instrument revoking a warrant must be signed by the eligible Judge, the nominated ART member or the chief officer of the law enforcement agency, as the case requires.

(4) If an eligible Judge or nominated ART member revokes a warrant, he or she must give a copy of the instrument of revocation to the chief officer of the law enforcement agency to which the law enforcement officer to whom the warrant was issued belongs or is seconded.

(5) 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, he or she must inform the chief officer of the law enforcement agency immediately.

Authorised Version C2025C00651 registered 28/11/2025

Division 4—Computer access warrants

27A Application for computer access warrant

Warrants sought for offence investigations

(1) A law enforcement officer (or another person on the law enforcement officer's behalf) may apply for the issue of a computer access warrant if the law enforcement officer suspects on reasonable grounds that:

(a) one or more relevant offences have been, are being, are about to be, or are likely to be, committed; and

(b) an investigation into those offences is being, will be, or is likely to be, conducted; and

(c) access to data held in a computer (the ***target computer***) is necessary, in the course of that investigation, for the purpose of enabling evidence to be obtained of:

(i) the commission of those offences; or

(ii) the identity or location of the offenders.

(2) If the application is being made by or on behalf of a State or Territory law enforcement officer, the reference in subsection (1) to a relevant offence does not include a reference to a State offence that has a federal aspect.

Warrants sought for recovery orders

(3) A law enforcement officer (or another person on the law enforcement officer's behalf) may apply for the issue of a computer access warrant if:

(a) a recovery order is in force; and

(b) the law enforcement officer suspects on reasonable grounds that access to data held in a computer (the ***target computer***) may assist in the location and safe recovery of the child to whom the recovery order relates.

Authorised Version C2025C00651 registered 28/11/2025

Warrants sought for international assistance investigations

(4) A law enforcement officer (or a person on the officer's behalf) may apply for the issue of a computer access warrant if the officer:

(a) is authorised to do so under an international assistance authorisation; and

(b) suspects on reasonable grounds that access to data held in a computer (the ***target computer***) is necessary, in the course of the investigation or investigative proceeding to which the authorisation relates, for the purpose of enabling evidence to be obtained of:

(i) the commission of an offence to which the authorisation relates; or

(ii) the identity or location of the persons suspected of committing the offence.

Warrants sought for integrity operations

(5) A federal law enforcement officer (or another person on the federal law enforcement officer's behalf) may apply for the issue of a computer access warrant if:

(a) an integrity authority is in effect authorising an integrity operation in relation to an offence that it is suspected has been, is being or is likely to be committed by a staff member of a target agency; and

(b) the federal law enforcement officer suspects on reasonable grounds that access to data held in a computer (the ***target computer***) will assist the conduct of the integrity operation by enabling evidence to be obtained relating to the integrity, location or identity of any staff member of the target agency.

Warrants sought for post-sentence order applications

(5A) A law enforcement officer (or another person on the officer's behalf) may apply for the issue of a computer access warrant if:

(a) a person is a terrorist offender in relation to whom an application for a post-sentence order could be made; and

(b) the person is detained in custody in a prison; and

Authorised Version C2025C00651 registered 28/11/2025

(c) the officer suspects on reasonable grounds that there is an appreciable risk of the person committing a serious Part 5.3 or 5.3A offence; and

(d) consideration is being given, will be given, or is likely to be given, by the AFP Minister (or a person on behalf of the AFP Minister), as to whether to apply for a post-sentence order in relation to the person; and

(e) the officer suspects on reasonable grounds that access to data held in a computer (the ***target computer***) would be likely to assist in determining whether to apply for the post-sentence order.

Warrants sought for Part 9.10 order applications

(5B) A law enforcement officer (or another person on the officer's behalf) may apply for the issue of a computer access warrant if:

(a) a person is a serious offender in relation to whom an application for a Part 9.10 order could be made; and

(b) the officer suspects on reasonable grounds that there is an appreciable risk of the person committing a serious violent or sexual offence; and

(c) consideration is being given, will be given, or is likely to be given, by the Immigration Minister (or a person on behalf of the Immigration Minister), as to whether to apply for a Part 9.10 order in relation to the person; and

(d) the officer suspects on reasonable grounds that access to data held in a computer (the ***target computer***) would be likely to assist in determining whether to apply for the Part 9.10 order.

Warrants sought for Part 5.3 supervisory orders

(6) A law enforcement officer (or another person on the officer's behalf) may apply for the issue of a computer access warrant if:

(a) a Part 5.3 supervisory order is in force in relation to a person; and

(b) the officer suspects on reasonable grounds that access to data held in a computer (the ***target computer***) to obtain

Authorised Version C2025C00651 registered 28/11/2025

information relating to the person would be likely to substantially assist in:

(i) achieving a Part 5.3 object; or

(ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with.

Note: For Part 5.3 supervisory orders that have been made but not come into force, see section 6C.

Warrants sought for community safety supervision orders

(6A) A law enforcement officer (or another person on the officer's behalf) may apply for the issue of a computer access warrant if:

(a) a community safety supervision order is in force in relation to a person; and

(b) the officer suspects on reasonable grounds that access to data held in a computer (the ***target computer***) to obtain information relating to the person would be likely to substantially assist in:

(i) achieving a Part 9.10 object; or

(ii) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with.

Note: For community safety supervision orders that have been made but not come into force, see section 6E.

Procedure for making applications

(7) An application under subsection (1), (3), (4), (5), (5A), (5B), (6) or (6A) may be made to an eligible Judge or to a nominated ART member.

(8) An application:

(a) must specify:

(i) the name of the applicant; and

(ii) the nature and duration of the warrant sought; and

Authorised Version C2025C00651 registered 28/11/2025

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

Unsworn applications—warrants sought for offence investigations

(9) If a law enforcement officer believes that:
(a) immediate access to data held in the target computer referred to in subsection (1) is necessary as described in paragraph (1)(c); and
(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made;
an application for a warrant under subsection (1) may be made before an affidavit is prepared or sworn.

(10) If subsection (9) applies, the applicant must:
(a) provide as much information as the eligible Judge or nominated ART member considers is reasonably practicable in the circumstances; and
(b) not later than 72 hours after the making of the application, send a duly sworn affidavit to the eligible Judge or nominated ART member, whether or not a warrant has been issued.

Unsworn applications—warrants sought for recovery orders

(11) If a law enforcement officer believes that:
(a) immediate access to data held in the target computer referred to in subsection (3) may assist as described in paragraph (3)(b); and
(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made;
an application for a warrant under subsection (3) may be made before an affidavit is prepared or sworn.

(12) If subsection (11) applies, the applicant must:
(a) provide as much information as the eligible Judge or nominated ART member considers is reasonably practicable in the circumstances; and

Authorised Version C2025C00651 registered 28/11/2025

(b) not later than 72 hours after the making of the application, send a duly sworn affidavit to the eligible Judge or nominated ART member, whether or not a warrant has been issued.

Unsworn applications—warrants sought for Part 5.3 supervisory orders

(13) If a law enforcement officer believes that:

(a) immediate access to data held in the target computer referred to in subsection (6) would be likely to substantially assist as described in paragraph (6)(b); and

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

an application for a warrant under subsection (6) may be made before an affidavit is prepared or sworn.

Unsworn applications—warrants sought for community safety supervision orders

(13A) If a law enforcement officer believes that:

(a) immediate access to data held in the target computer referred to in subsection (6A) would be likely to substantially assist as described in paragraph (6A)(b); and

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

an application for a warrant under subsection (6A) may be made before an affidavit is prepared or sworn.

Applicant must provide information

(14) If subsection (13) or (13A) applies, the applicant must:

(a) provide as much information as the eligible Judge or nominated ART member considers is reasonably practicable in the circumstances; and

(b) not later than 72 hours after the making of the application, send a duly sworn affidavit to the eligible Judge or

Authorised Version C2025C00651 registered 28/11/2025

nominated ART member, whether or not a warrant has been issued.

Target computer

(15) The target computer referred to in subsection (1), (3), (4), (5), (5A), (5B), (6) or (6A) may be any one or more of the following:
  (a) a particular computer;
  (b) a computer on particular premises;
  (c) a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).

27B Remote application

(1) If a law enforcement officer believes that it is impracticable for an application for a computer access warrant to be made in person, the application may be made under section 27A 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 transmit a copy of the affidavit, whether sworn or unsworn, to the eligible Judge or to the nominated ART member who is to determine the application.

27C Determining the application

(1) An eligible Judge or a nominated ART member may issue a computer access warrant if satisfied:
  (a) in the case of a warrant sought in relation to a relevant offence—that there are reasonable grounds for the suspicion founding the application for the warrant; and
  (b) in the case of a warrant sought in relation to a recovery order—that such an order is in force and that there are reasonable grounds for the suspicion founding the application for the warrant; and
  (c) in the case of a warrant sought in relation to an international assistance authorisation—that such an authorisation is in

Authorised Version C2025C00651 registered 28/11/2025

force and that there are reasonable grounds for the suspicion founding the application for the warrant; and

(d) in the case of a warrant sought for the purposes of an integrity operation—that the integrity authority for the operation is in effect, and that there are reasonable grounds for the suspicions founding the application for the warrant (as mentioned in paragraphs 27A(5)(a) and (b)); and

(da) in the case of a computer access warrant sought to determine whether to apply for a post-sentence order—that the conditions in paragraphs 27A(5A)(a), (b) and (d) are met, and there are reasonable grounds for the suspicions founding the application for the warrant (as mentioned in paragraphs 27A(5A)(c) and (e)); and

(db) in the case of a computer access warrant sought to determine whether to apply for a Part 9.10 order—that the conditions in paragraphs 27A(5B)(a) and (c) are met, and there are reasonable grounds for the suspicions founding the application for the warrant (as mentioned in paragraphs 27A(5B)(b) and (d)); and

(e) in the case of a computer access warrant sought in relation to a Part 5.3 supervisory order that is in force in relation to a person—that the order is in force in relation to the person, and there are reasonable grounds for the suspicion founding the application for the warrant (as mentioned in paragraph 27A(6)(b)); and

(ea) in the case of a computer access warrant sought in relation to a community safety supervision order that is in force in relation to a person—that the order is in force in relation to the person, and there are reasonable grounds for the suspicion founding the application for the warrant (as mentioned in paragraph 27A(6A)(b)); and

(f) in the case of an unsworn application—that it would have been impracticable for an affidavit to have been sworn or prepared before the application was made; and

(g) in the case of a remote application—that it would have been impracticable for the application to have been made in person.

Authorised Version C2025C00651 registered 28/11/2025

Note: For Part 5.3 supervisory orders that have been made but not come into force, see section 6C. For community safety supervision orders that have been made but not come into force, see section 6E.

(2) In determining whether a computer access warrant should be issued, the eligible Judge or nominated ART member must have regard to:

(a) in the case of a warrant sought in relation to a relevant offence or an international assistance authorisation, or for the purposes of an integrity operation—the nature and gravity of the alleged offence; and

(b) in the case of a warrant sought to assist in the location and safe recovery of a child to whom a recovery order relates—the circumstances that gave rise to the making of the order; and

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

(d) the existence of any alternative means of obtaining the evidence or information sought to be obtained; and

(e) in the case of a warrant sought in relation to a relevant offence or a recovery order, or for the purposes of an integrity operation—the likely evidentiary or intelligence value of any evidence or information sought to be obtained; and

(f) in the case of a warrant sought in relation to an international assistance authorisation—the likely evidentiary or intelligence value of any evidence or information sought to be obtained, to the extent that this is possible to determine from information obtained from the international entity to which the authorisation relates; and

(j) in the case of a warrant sought in relation to a relevant offence or a recovery order—any previous warrant sought or issued under this Division in connection with the same alleged offence or the same recovery order.

(3) In addition to the matters in subsection (2), in determining whether to issue a computer access warrant sought to determine whether to

Authorised Version C2025C00651 registered 28/11/2025

apply for a post-sentence order in relation to a person, the eligible Judge or nominated ART member must have regard to:

(a) the likely value of the information sought to be obtained in determining whether to apply for the post-sentence order; and

(b) any previous application for a computer access warrant sought or issued to determine whether to apply for a post-sentence order in relation to the person.

(4) In addition to the matters in subsection (2), in determining whether to issue a computer access warrant sought in a case where a Part 5.3 supervisory order is in force in relation to a person, the eligible Judge or nominated ART member must have regard to:

(a) the likely value of the information sought to be obtained, in:

(i) achieving a Part 5.3 object; or

(ii) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and

(b) whether the access to the data in accordance with the warrant would be the means of obtaining the evidence or information sought to be obtained, that is likely to have the least interference with any person's privacy; and

(c) if the order is a control order:

(i) the possibility that the person has engaged, is engaging, or will engage, in a terrorist act; or

(ii) the possibility that the person has provided, is providing, or will provide, support for a terrorist act; or

(iii) the possibility that the person has facilitated, is facilitating, or will facilitate, a terrorist act; or

(iv) the possibility that the person has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country; or

(v) the possibility that the person has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country; and

(d) if the order is an extended supervision order or interim supervision order—the possibility that the person has

Authorised Version C2025C00651 registered 28/11/2025

committed, is committing, or will commit, a serious Part 5.3 or 5.3A offence; and

(e) in relation to any Part 5.3 supervisory order—the possibility that the person has contravened, is contravening, or will contravene, the order or a succeeding Part 5.3 supervisory order; and

(f) any previous computer access warrant sought or issued on the basis of a Part 5.3 supervisory order that is or was in force in relation to the person.

(5) In addition to the matters in subsection (2), in determining whether to issue a computer access warrant sought to determine whether to apply for a Part 9.10 order in relation to a person, the eligible Judge or nominated ART member must have regard to:

(a) the likely value of the information sought to be obtained in determining whether to apply for the Part 9.10 order; and

(b) any previous application for a computer access warrant sought or issued to determine whether to apply for a Part 9.10 order in relation to the person.

(6) In addition to the matters in subsection (2), in determining whether to issue a computer access warrant sought in a case where a community safety supervision order is in force in relation to a person, the eligible Judge or nominated ART member must have regard to:

(a) the likely value of the information sought to be obtained, in:

(i) achieving a Part 9.10 object; or

(ii) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with; and

(b) whether the access to the data in accordance with the warrant would be the means of obtaining the evidence or information sought to be obtained, that is likely to have the least interference with any person's privacy; and

(c) the possibility that the person has committed, is committing, or will commit, a serious violent or sexual offence; and

Authorised Version C2025C00651 registered 28/11/2025

(d) the possibility that the person has contravened, is contravening, or will contravene, the community safety supervision order or a succeeding community safety supervision order; and

(e) any previous computer access warrant sought or issued on the basis of a community safety supervision order that is or was in force in relation to the person.

27D What must a computer access warrant contain?

(1) A computer access warrant must:

(a) state that the eligible Judge or nominated ART member issuing the warrant is satisfied of the matters referred to in subsection 27C(1) and has had regard to the matters referred to in subsections 27C(2), (3), (4), (5) and (6) (as the case requires); and

(b) specify:

(i) the name of the applicant; and

(ii) if the warrant relates to one or more alleged relevant offences—the alleged offences in respect of which the warrant is issued; and

(iii) if the warrant relates to a recovery order—the date the order was made and the name of the child to whom the order relates; and

(iv) if the warrant relates to an international assistance authorisation—each offence to which the authorisation relates; and

(v) if the warrant is issued for the purposes of an integrity operation—the integrity authority for the operation and each alleged relevant offence in relation to which the authority was granted; and

(vi) the date the warrant is issued; and

(vii) if the target computer is or includes a particular computer—the computer; and

(viii) if the target computer is or includes a computer on particular premises—the premises; and

Authorised Version C2025C00651 registered 28/11/2025

(ix) if the target computer is or includes a computer associated with, used by or likely to be used by, a person—the person (whether by name or otherwise); and

(x) the period during which the warrant is in force (see subsection (3)); and

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

(xii) any conditions subject to which things may be done under the warrant.

(1A) If a computer access warrant is issued to determine whether to apply for a post-sentence order in relation to a person, the warrant must also specify the name of the person.

(2) If a computer access warrant is issued on the basis of a Part 5.3 supervisory order that is in force in relation to a person, the warrant must also specify the following details:

(a) the name of the person;

(b) the date the Part 5.3 supervisory order was made;

(c) if (disregarding section 6C) the order is not already in force and the order is not an interim control order—when the order comes into force;

(d) whether the order is:

(i) an interim control order; or

(ii) a confirmed control order; or

(iii) an interim supervision order; or

(iv) an extended supervision order.

(2A) If a computer access warrant is issued to determine whether to apply for a Part 9.10 order in relation to a person, the warrant must also specify the name of the person.

(2B) If a computer access warrant is issued on the basis of a community safety supervision order that is in force in relation to a person, the warrant must also specify the following details:

(a) the name of the person;

Authorised Version C2025C00651 registered 28/11/2025

(b) the date the community safety supervision order was made;

(c) if (disregarding section 6E) the order is not already in force—when the order comes into force.

(3) A warrant may only be issued:

(a) for a period of no more than 90 days; or

(b) if the warrant is issued for the purposes of an integrity operation—for a period of no more than 21 days.

Note: The access to data held in the target computer pursuant to a warrant may be discontinued earlier—see section 27H.

(3A) To avoid doubt, a warrant issued on the basis that a Part 5.3 supervisory order is in force remains in force for the period mentioned in paragraph (3)(a) even if the order ceases to be in force, provided that the order is replaced by a succeeding Part 5.3 supervisory order.

Note 1: If there is no succeeding Part 5.3 supervisory order, the warrant must be revoked (see section 27H).

Note 2: A control order is not a succeeding Part 5.3 supervisory order in relation to an extended supervision order, and vice versa (see section 6D).

(3B) To avoid doubt, a warrant issued on the basis that a community safety supervision order is in force remains in force for the period mentioned in paragraph (3)(a) even if the order ceases to be in force, provided that the order is replaced by a succeeding community safety supervision order.

Note: If there is no succeeding community safety supervision order, the warrant must be revoked (see section 27H).

(4) In the case of a warrant authorising the access to data held in the target computer on premises that are vehicles, the warrant need only specify the class of vehicle in relation to which the access to data held in the target computer is authorised.

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

Authorised Version C2025C00651 registered 28/11/2025

(6) As soon as practicable after completing and signing a warrant issued on a remote application, the person issuing it must:

(a) inform the applicant of:

(i) the terms of the warrant; and

(ii) the date on which, and the time at which, the warrant was issued; and

(b) give the warrant to the applicant while retaining a copy of the warrant for the person's own record.

27E What a computer access warrant authorises

(1) A computer access warrant must authorise the doing of specified things (subject to any restrictions or conditions specified in the warrant) in relation to the relevant target computer.

(2) The things that may be specified are any of the following that the eligible Judge or nominated ART member considers appropriate in the circumstances:

(a) entering specified premises for the purposes of doing the things mentioned in this subsection;

(b) entering any premises for the purposes of gaining entry to, or exiting, the specified premises;

(c) using:

(i) the target computer; or

(ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or

(iii) any other electronic equipment; or

(iv) a data storage device;

for the purpose of obtaining access to data (the ***relevant data***) that is held in the target computer at any time while the warrant is in force, in order to determine whether the relevant data is covered by the warrant;

(d) if necessary to achieve the purpose mentioned in paragraph (c)—adding, copying, deleting or altering other data in the target computer;

Authorised Version C2025C00651 registered 28/11/2025

(e) if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so:

(i) using any other computer or a communication in transit to access the relevant data; and

(ii) if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;

(f) removing a computer or other thing from premises for the purposes of doing any thing specified in the warrant in accordance with this subsection, and returning the computer or other thing to the premises;

(g) copying any data to which access has been obtained, and that:

(i) appears to be relevant for the purposes of determining whether the relevant data is covered by the warrant; or

(ii) is covered by the warrant;

(h) intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing specified in the warrant in accordance with this subsection;

(i) any other thing reasonably incidental to any of the above.

Note: As a result of the warrant, a person who, by means of a telecommunications facility, obtains access to data stored in a computer etc. will not commit an offence under Part 10.7 of the *Criminal Code* or equivalent State or Territory laws (provided that the person acts within the authority of the warrant).

(2A) If:

(a) a computer access warrant authorises the removal of a computer or other thing from premises as mentioned in paragraph (2)(f); and

(b) a computer or thing is removed from the premises in accordance with the warrant;

the computer or thing must be returned to the premises within a reasonable period.

Authorised Version C2025C00651 registered 28/11/2025

(3) For the purposes of paragraph (2)(g), if:

(a) access has been obtained to data; and

(b) the data is subject to a form of electronic protection;

the data is taken to be relevant for the purposes of determining whether the relevant data is covered by the warrant.

When data is covered by a warrant

(4) For the purposes of this section, data is ***covered by*** a warrant if:

(a) in the case of a warrant sought in relation to a relevant offence—access to the data is necessary as described in paragraph 27A(1)(c); or

(b) in the case of a warrant sought in relation to a recovery order—access to the data may assist as described in paragraph 27A(3)(b); or

(c) in the case of a warrant sought in relation to an international assistance authorisation—access to the data is necessary as described in paragraph 27A(4)(b); or

(d) in the case of a warrant sought for the purposes of an integrity operation—access to the data will assist as described in paragraph 27A(5)(b); or

(da) in the case of a warrant sought to determine whether to apply for a post-sentence order—access to the data would be likely to assist as described in paragraph 27A(5A)(e); or

(e) in the case of a warrant issued on the basis of a Part 5.3 supervisory order that is in force in relation to a person—access to the data would be likely to substantially assist as described in paragraph 27A(6)(b); or

(f) in the case of a warrant sought to determine whether to apply for a Part 9.10 order—access to the data would be likely to assist as described in paragraph 27A(5B)(d); or

(g) in the case of a warrant issued on the basis of a community safety supervision order that is in force in relation to a person—access to the data would be likely to substantially assist as described in paragraph 27A(6A)(b).

Authorised Version C2025C00651 registered 28/11/2025

Certain acts not authorised

(5) Subsection (2) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer;

unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified in the warrant; or

(b) cause any other material loss or damage to other persons lawfully using a computer.

Warrant must provide for certain matters

(6) A computer access warrant must:

(a) authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant; and

(b) if the warrant authorises entering premises—state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.

Concealment of access etc.

(7) If any thing has been done in relation to a computer under:

(a) a computer access warrant; or

(b) this subsection;

then, in addition to the things specified in the warrant, the warrant authorises the doing of any of the following:

(c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant or under this subsection;

(d) entering any premises where the computer is reasonably believed to be, for the purposes of doing the things mentioned in paragraph (c);

Authorised Version C2025C00651 registered 28/11/2025

(e) entering any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (d);

(f) removing the computer or another thing from any place where it is situated for the purposes of doing the things mentioned in paragraph (c), and returning the computer or other thing to that place;

(g) if, having regard to other methods (if any) of doing the things mentioned in paragraph (c) which are likely to be as effective, it is reasonable in all the circumstances to do so:

(i) using any other computer or a communication in transit to do those things; and

(ii) if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;

(h) intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing mentioned in this subsection;

(i) any other thing reasonably incidental to any of the above;

at the following time:

(j) at any time while the warrant is in force or within 28 days after it ceases to be in force;

(k) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (j)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).

(8) Subsection (7) does not authorise the doing of a thing that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer;

unless the doing of the thing is necessary to do one or more of the things specified in subsection (7); or

(b) cause any other material loss or damage to other persons lawfully using a computer.

Authorised Version C2025C00651 registered 28/11/2025

(9) If a computer or another thing is removed from a place in accordance with paragraph (7)(f), the computer or thing must be returned to the place within a reasonable period.

27F Extension and variation of computer access warrant

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

(a) for an extension of the warrant for a period of no more than:

(i) 90 days after the day the warrant would otherwise expire; or

(ii) if the warrant is issued for the purposes of an integrity operation—21 days after the day the warrant would otherwise expire; or

(b) for a variation of any of the other terms of the warrant.

(2) The application is to be made to an eligible Judge or to a nominated ART member and must be accompanied by the original warrant.

(3) Sections 27A and 27B apply, with any necessary changes, to an application under this section as if it were an application for the warrant.

(4) The eligible Judge or nominated ART member may grant an application if satisfied that the matters referred to in subsection 27C(1) still exist, having regard to the matters in subsections 27C(2), (3), (4), (5) and (6) (as the case requires).

(5) If the eligible Judge or nominated ART member grants the application, the eligible Judge or nominated ART member must endorse the new expiry date or the other varied term on the original warrant.

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

Authorised Version C2025C00651 registered 28/11/2025

27G Revocation of computer access warrant

(1) A computer access warrant may, by instrument in writing, be revoked by an eligible Judge or nominated ART member on the initiative of the eligible Judge or nominated ART member at any time before the expiration of the period of validity specified in the warrant.

(2) If the circumstances set out in subsection 27H(2), (3) or (4) apply in relation to a computer access warrant, the chief officer of the law enforcement agency to which the law enforcement officer to whom the warrant was issued belongs or is seconded must, by instrument in writing, revoke the warrant.

(3) The instrument revoking a warrant must be signed by the eligible Judge, the nominated ART member or the chief officer of the law enforcement agency, as the case requires.

(4) If an eligible Judge or nominated ART member revokes a warrant, the eligible Judge or nominated ART member must give a copy of the instrument of revocation to the chief officer of the law enforcement agency to which the law enforcement officer to whom the warrant was issued belongs or is seconded.

(5) If:

(a) an eligible Judge or nominated ART member revokes a warrant; and

(b) at the time of the revocation, a law enforcement officer is executing the warrant;

the law enforcement officer is not subject to any civil or criminal liability for any act done in the proper execution of that warrant before the officer is made aware of the revocation.

27H Discontinuance of access under warrant

Scope

(1) This section applies if a computer access warrant is issued to a law enforcement officer.

Authorised Version C2025C00651 registered 28/11/2025

Obligations on chief officers

(2) If:

(a) the computer access warrant has been sought by or on behalf of a law enforcement officer; and

(b) the chief officer of the law enforcement agency to which the law enforcement officer belongs or is seconded is satisfied that:

(i) access to data under the warrant is no longer required for the purpose for which it was sought; or

(ii) without limiting subparagraph (i), if the warrant was sought for the purposes of an integrity operation—the integrity authority for the integrity operation is no longer in effect; and

(c) the warrant was not issued to determine whether to apply for a post-sentence order; and

(d) the warrant was not issued to determine whether to apply for a Part 9.10 order;

the chief officer must (subject to subsections (3) and (4)), in addition to revoking the warrant under section 27G, take the steps necessary to ensure that access to data authorised by the warrant is discontinued.

(3) The chief officer is required to take steps under subsection (2) in relation to a computer access warrant that is issued on the basis of a Part 5.3 supervisory order that was in force in relation to a person only if neither the Part 5.3 supervisory order, nor any succeeding Part 5.3 supervisory order, is in force in relation to the person.

Note: A control order is not a succeeding Part 5.3 supervisory order in relation to an extended supervision order, and vice versa (see section 6D).

(4) The chief officer is required to take steps under subsection (2) in relation to a computer access warrant that is issued on the basis of a community safety supervision order that was in force in relation to a person only if neither the community safety supervision order, nor any succeeding community safety supervision order, is in force in relation to the person.

Authorised Version C2025C00651 registered 28/11/2025

(8) If the chief officer of a law enforcement agency is notified that a warrant has been revoked by an eligible Judge or a nominated ART member under section 27G, the chief officer must take the steps necessary to ensure that access to data authorised by the warrant is discontinued as soon as practicable.

Obligations on law enforcement officers to whom warrants are issued etc.

(9) If the law enforcement officer to whom the warrant is issued, or who is primarily responsible for executing the warrant, believes that:

(a) access to data under the warrant is no longer necessary for the purpose for which it was sought; or

(b) without limiting paragraph (a), if the warrant was sought for the purposes of an integrity operation—the integrity authority for the integrity operation is no longer in effect;

the law enforcement officer must (subject to subsection (10)) immediately inform the chief officer of the law enforcement agency to which the law enforcement officer belongs or is seconded.

(10) If the law enforcement officer to whom a warrant is issued, or who is primarily responsible for executing a warrant issued, on the basis that a Part 5.3 supervisory order was in force in relation to a person believes that neither the Part 5.3 supervisory order, nor any succeeding Part 5.3 supervisory order, is in force in relation to the person, the officer must immediately inform the chief officer of the law enforcement agency to which the officer belongs or is seconded.

(11) If the law enforcement officer to whom a warrant is issued, or who is primarily responsible for executing a warrant issued, on the basis that a community safety supervision order was in force in relation to a person believes that neither the community safety supervision order, nor any succeeding community safety supervision order, is in force in relation to the person, the officer must immediately

Authorised Version C2025C00651 registered 28/11/2025

inform the chief officer of the law enforcement agency to which the officer belongs or is seconded.

27J Relationship of this Division to parliamentary privileges and immunities

To avoid doubt, this Division does not affect the law relating to the powers, privileges and immunities of any of the following:

(a) each House of the Parliament;

(b) the members of each House of the Parliament;

(c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

Authorised Version C2025C00651 registered 28/11/2025

Division 5—Data disruption warrants

27KAA Sunsetting

This Division ceases to have effect 5 years after it commences.

27KA Application for data disruption warrant

(1) A law enforcement officer of the Australian Federal Police or the Australian Crime Commission (or another person on the law enforcement officer's behalf) may apply for the issue of a data disruption warrant if the law enforcement officer suspects on reasonable grounds that:

(a) one or more relevant offences of a particular kind have been, are being, are about to be, or are likely to be, committed; and

(b) those offences involve, or are likely to involve, data held in a computer (the ***target computer***); and

(c) disruption of data held in the target computer is likely to substantially assist in frustrating the commission of one or more relevant offences that:

(i) involve, or are likely to involve, data held in the target computer; and

(ii) are of the same kind as the relevant offences referred to in paragraph (a).

Procedure for making applications

(2) An application under subsection (1) may be made to an eligible Judge or to a nominated ART member.

(3) An application:

(a) must specify:

(i) the name of the applicant; and

(ii) the nature and duration of the warrant sought; and

(b) subject to this section, must be supported by an affidavit setting out:

Authorised Version C2025C00651 registered 28/11/2025

(i) the grounds on which the warrant is sought; and
(ii) the things proposed to be authorised by the warrant in accordance with section 27KE; and
(iii) an assessment of how disruption of data held in the target computer is likely to substantially assist as described in paragraph (1)(c), to the extent that such an assessment is possible; and
(iv) an assessment of the likelihood that disruption of data held in the target computer will substantially assist as described in paragraph (1)(c), to the extent that such an assessment is possible.

Unsworn applications

(4) If a law enforcement officer believes that:
(a) immediate disruption of data held in the target computer referred to in subsection (1) is likely to substantially assist as described in paragraph (1)(c); and
(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made;
an application for a warrant under subsection (1) may be made before an affidavit is prepared or sworn.

(5) If subsection (4) applies, the applicant must:
(a) provide as much information as the eligible Judge or nominated ART member considers is reasonably practicable in the circumstances; and
(b) not later than 72 hours after the making of the application, send a duly sworn affidavit to the eligible Judge or nominated ART member, whether or not a warrant has been issued.

Target computer

(6) The target computer referred to in subsection (1) may be any one or more of the following:
(a) a particular computer;

Authorised Version C2025C00651 registered 28/11/2025

(b) a computer on particular premises;

(c) a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).

27KB Remote application

(1) If a law enforcement officer believes that it is impracticable for an application for a data disruption warrant to be made in person, the application may be made under section 27KA 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 transmit a copy of the affidavit, whether sworn or unsworn, to the eligible Judge or to the nominated ART member who is to determine the application.

27KBA Endorsement of application—Australian Federal Police

(1) A law enforcement officer of the Australian Federal Police (or another person on the law enforcement officer's behalf) must not make an application for the issue of a data disruption warrant unless the making of the application has been endorsed, either orally or in writing, by an endorsing officer of the Australian Federal Police.

(2) An endorsing officer of the Australian Federal Police must not endorse the making of an application for the issue of a data disruption warrant unless the endorsing officer is satisfied that the making of the application is appropriate in all the circumstances.

(3) For the purposes of this section, an ***endorsing officer*** of the Australian Federal Police means:

(a) a law enforcement officer of the Australian Federal Police who is declared, in writing, by the chief officer of the Australian Federal Police to be an endorsing officer of the Australian Federal Police; or

(b) a person who is in a class of law enforcement officers of the Australian Federal Police that is declared, in writing, by the

Authorised Version C2025C00651 registered 28/11/2025

chief officer of the Australian Federal Police to be a class of endorsing officers of the Australian Federal Police.

(4) The chief officer of the Australian Federal Police must not make a declaration under paragraph (3)(a) in relation to a law enforcement officer of the Australian Federal Police unless:

(a) the law enforcement officer is a superintendent, or a person holding a higher rank, in the Australian Federal Police; and

(b) the chief officer is satisfied that the law enforcement officer has the relevant skills, knowledge and experience to endorse the making of applications for the issue of data disruption warrants; and

(c) the chief officer is satisfied that the law enforcement officer has completed all current internal training requirements relating to endorsing the making of applications for the issue of data disruption warrants.

(5) The chief officer of the Australian Federal Police must not make a declaration under paragraph (3)(b) in relation to a class of law enforcement officers of the Australian Federal Police unless:

(a) each person in that class is a superintendent, or a person holding a higher rank, in the Australian Federal Police; and

(b) the chief officer is satisfied that each person in that class has the relevant skills, knowledge and experience to endorse the making of applications for the issue of data disruption warrants; and

(c) the chief officer is satisfied that each person in that class has completed all current internal training requirements relating to endorsing the making of applications for the issue of data disruption warrants.

(6) A declaration under this section is not a legislative instrument.

27KBB Endorsement of application—Australian Crime Commission

(1) A law enforcement officer of the Australian Crime Commission (or another person on the law enforcement officer's behalf) must not make an application for the issue of a data disruption warrant

Authorised Version C2025C00651 registered 28/11/2025

unless the making of the application has been endorsed, either orally or in writing, by an endorsing officer of the Australian Crime Commission.

(2) An endorsing officer of the Australian Crime Commission must not endorse the making of an application for the issue of a data disruption warrant unless the endorsing officer is satisfied that the making of the application is appropriate in all the circumstances.

(3) For the purposes of this section, an ***endorsing officer*** of the Australian Crime Commission means:

(a) a law enforcement officer of the Australian Crime Commission who is declared, in writing, by the chief officer of the Australian Crime Commission to be an endorsing officer of the Australian Crime Commission; or

(b) a person who is in a class of law enforcement officers of the Australian Crime Commission that is declared, in writing, by the chief officer of the Australian Crime Commission to be a class of endorsing officers of the Australian Crime Commission.

(4) The chief officer of the Australian Crime Commission must not make a declaration under paragraph (3)(a) in relation to a law enforcement officer of the Australian Crime Commission unless:

(a) the law enforcement officer is an executive level member of the staff of the Australian Crime Commission; and

(b) the chief officer is satisfied that the law enforcement officer has the relevant skills, knowledge and experience to endorse the making of applications for the issue of data disruption warrants; and

(c) the chief officer is satisfied that the law enforcement officer has completed all current internal training requirements relating to endorsing the making of applications for the issue of data disruption warrants.

(5) The chief officer of the Australian Crime Commission must not make a declaration under paragraph (3)(b) in relation to a class of

Authorised Version C2025C00651 registered 28/11/2025

law enforcement officers of the Australian Crime Commission unless:

(a) each person in that class is an executive level member of the staff of the Australian Crime Commission; and

(b) the chief officer is satisfied that each person in that class has the relevant skills, knowledge and experience to endorse the making of applications for the issue of data disruption warrants; and

(c) the chief officer is satisfied that each person in that class has completed all current internal training requirements relating to endorsing the making of applications for the issue of data disruption warrants.

(6) A declaration under this section is not a legislative instrument.

27KC Determining the application

(1) An eligible Judge or a nominated ART member may issue a data disruption warrant if satisfied:

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

(b) the disruption of data authorised by the warrant is reasonably necessary and proportionate, having regard to the offences referred to in paragraph 27KA(1)(c); and

(c) in the case of an unsworn application—that it would have been impracticable for an affidavit to have been sworn or prepared before the application was made; and

(d) in the case of a remote application—that it would have been impracticable for the application to have been made in person.

(2) In determining whether a data disruption warrant should be issued, the eligible Judge or nominated ART member must have regard to:

(a) the nature and gravity of the conduct constituting the offences referred to in paragraph 27KA(1)(c); and

Authorised Version C2025C00651 registered 28/11/2025

(b) the likelihood that the disruption of data authorised by the warrant will frustrate the commission of the offences referred to in paragraph 27KA(1)(c); and

(c) the existence of any alternative means of frustrating the commission of the offences referred to in paragraph 27KA(1)(c); and

(ca) the nature of the things proposed to be authorised by the warrant in accordance with section 27KE; and

(cb) the extent to which the execution of the warrant is likely to result in access to, or disruption of, data of persons lawfully using a computer, and any privacy implications (to the extent known) resulting from that access or disruption; and

(cc) any steps that are proposed to be taken to avoid or minimise the extent to which the execution of the warrant is likely to impact on persons lawfully using a computer; and

(cd) the extent to which the execution of the warrant is likely to cause a person to suffer a temporary loss of:

(i) money; or

(ii) digital currency; or

(iii) property (other than data);

so far as that matter is known to the eligible Judge or nominated ART member; and

(ce) if:

(i) the eligible Judge or nominated ART member believes on reasonable grounds that the data covered by the warrant (within the meaning of section 27KE) is data of a person who is working in a professional capacity as a journalist or of an employer of such a person; and

(ii) each of the offences referred to in paragraph 27KA(1)(c) is an offence against a secrecy provision;

whether the public interest in issuing the warrant outweighs:

(iii) the public interest in protecting the confidentiality of the identity of the journalist's source; and

(iv) the public interest in facilitating the exchange of information between journalists and members of the

Authorised Version C2025C00651 registered 28/11/2025

public so as to facilitate reporting of matters in the public interest; and

(d) any previous warrant sought or issued under this Division in relation to the alleged relevant offences referred to in paragraph 27KA(1)(c).

(3) For the purposes of having regard to the nature and gravity of the conduct constituting the offences referred to in paragraph 27KA(1)(c), the eligible Judge or a nominated ART member must give weight to the following matters:

(a) whether that conduct amounts to:

(i) an activity against the security of the Commonwealth; or

(ii) an offence against Chapter 5 of the *Criminal Code*;

(b) whether that conduct amounts to:

(i) an activity against the proper administration of Government; or

(ii) an offence against Chapter 7 of the *Criminal Code*;

(c) whether that conduct:

(i) causes, or has the potential to cause, serious violence, or serious harm, to a person; or

(ii) amounts to an offence against Chapter 8 of the *Criminal Code*;

(d) whether that conduct:

(i) causes, or has the potential to cause, a danger to the community; or

(ii) amounts to an offence against Chapter 9 of the *Criminal Code*;

(e) whether that conduct:

(i) causes, or has the potential to cause, substantial damage to, or loss of, data, property or critical infrastructure; or

(ii) amounts to an offence against Chapter 10 of the *Criminal Code*;

(f) whether that conduct involves, or is related to, the commission of:

Authorised Version C2025C00651 registered 28/11/2025

(i) transnational crime; or
(ii) serious crime; or
(iii) organised crime;
that is not covered by any of the preceding paragraphs.

(4) Subsection (3) does not limit the matters that may be considered by the eligible Judge or nominated ART member.

(5) To avoid doubt, this Act does not prevent a data disruption warrant from being issued in a case where the conduct constituting the offences referred to in paragraph 27KA(1)(c) is not covered by subsection (3).

(6) For the purposes of this section, ***secrecy provision*** means a provision of a law of the Commonwealth or of a State that prohibits:
(a) the communication, divulging or publication of information; or
(b) the production of, or the publication of the contents of, a document.

27KD What must a data disruption warrant contain?

(1) A data disruption warrant must:
(a) state that the eligible Judge or nominated ART member issuing the warrant is satisfied of the matters referred to in subsection 27KC(1) and has had regard to the matters referred to in subsection 27KC(2); and
(b) specify:
(i) the name of the applicant; and
(ii) the alleged relevant offences referred to in paragraph 27KA(1)(c); and
(iii) the date the warrant is issued; and
(iv) if the target computer is or includes a particular computer—the computer; and
(v) if the target computer is or includes a computer on particular premises—the premises; and

Authorised Version C2025C00651 registered 28/11/2025

(vi) if the target computer is or includes a computer associated with, used by or likely to be used by, a known person—the person (whether by name or otherwise); and

(vii) the period during which the warrant is in force (see subsection (2)); and

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

(ix) any conditions subject to which things may be done under the warrant.

(2) A warrant may only be issued for a period of no more than 90 days.

Note: The access to, or disruption of, data held in the target computer pursuant to a warrant may be discontinued earlier—see section 27KH.

(3) In the case of a warrant authorising access to, or disruption of, data held in the target computer on premises that are vehicles, the warrant need only specify the class of vehicle in relation to which the access to, and disruption of, data held in the target computer is authorised.

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

(5) As soon as practicable after completing and signing a warrant issued on a remote application, the person issuing it must:

(a) inform the applicant of:

(i) the terms of the warrant; and

(ii) the date on which, and the time at which, the warrant was issued; and

(b) give the warrant to the applicant while retaining a copy of the warrant for the person's own record.

Authorised Version C2025C00651 registered 28/11/2025

27KE What a data disruption warrant authorises

(1) A data disruption warrant must authorise the doing of specified things (subject to any restrictions or conditions specified in the warrant) in relation to the relevant target computer.

(2) The things that may be specified are any of the following that the eligible Judge or nominated ART member considers appropriate in the circumstances:

(a) entering specified premises for the purposes of doing the things mentioned in this subsection;

(b) entering any premises for the purposes of gaining entry to, or exiting, the specified premises;

(c) using:

(i) the target computer; or

(ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or

(iii) any other electronic equipment; or

(iv) a data storage device;

for the following purposes:

(v) obtaining access to data (the ***relevant data***) that is held in the target computer at any time while the warrant is in force, in order to determine whether the relevant data is covered by the warrant;

(vi) disrupting the relevant data at any time while the warrant is in force, if doing so is likely to assist in frustrating the commission of one or more relevant offences covered by the warrant;

(d) if necessary to achieve the purpose mentioned in subparagraph (c)(v) or (vi)—adding, copying, deleting or altering other data in the target computer;

(e) if, having regard to other methods (if any) of obtaining access to, or disrupting, the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so:

Authorised Version C2025C00651 registered 28/11/2025

(i) using any other computer or a communication in transit to access or disrupt the relevant data; and

(ii) if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;

(f) removing a computer or other thing from premises for the purposes of doing any thing specified in the warrant in accordance with this subsection, and returning the computer or other thing to the premises;

(g) copying any data to which access has been obtained, and that:

(i) appears to be relevant for the purposes of determining whether the relevant data is covered by the warrant; or

(ii) is covered by the warrant;

(h) intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing specified in the warrant in accordance with this subsection;

(i) any other thing reasonably incidental to any of the above.

Note: As a result of the warrant, a person who, by means of a telecommunications facility, obtains access to data stored in a computer etc. will not commit an offence under Part 10.7 of the *Criminal Code* or equivalent State or Territory laws (provided that the person acts within the authority of the warrant).

(3) If:

(a) a data disruption warrant authorises the removal of a computer or other thing from premises as mentioned in paragraph (2)(f); and

(b) a computer or thing is removed from the premises in accordance with the warrant;

the computer or thing must be returned to the premises as soon as is reasonably practicable to do so once the computer or thing is no longer required for the purposes of doing any thing authorised by the warrant.

(4) For the purposes of paragraph (2)(g), if:

Authorised Version C2025C00651 registered 28/11/2025

(a) access has been obtained to data; and

(b) the data is subject to a form of electronic protection;

the data is taken to be relevant for the purposes of determining whether the relevant data is covered by the warrant.

When data is covered by a warrant

(5) For the purposes of this section, data is ***covered by*** a warrant if disruption of the data is likely to substantially assist as described in paragraph 27KA(1)(c).

When a relevant offence is covered by a warrant

(6) For the purposes of this section, a relevant offence is ***covered by*** a warrant if the relevant offence is referred to in paragraph 27KA(1)(c).

Certain acts not authorised

(7) Subsection (2) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer;

unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified in the warrant; or

(b) cause any other material loss or damage to other persons lawfully using a computer, unless the loss or damage is reasonably necessary, and proportionate, to do one or more of the things specified in the warrant.

Warrant must provide for certain matters

(8) A data disruption warrant must:

(a) authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant; and

Authorised Version C2025C00651 registered 28/11/2025

(b) if the warrant authorises entering premises—state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.

Concealment of access etc.

(9) If any thing has been done in relation to a computer under:

(a) a data disruption warrant; or

(b) this subsection;

then, in addition to the things specified in the warrant, the warrant authorises the doing of any of the following:

(c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant or under this subsection;

(d) entering any premises where the computer is reasonably believed to be, for the purposes of doing the things mentioned in paragraph (c);

(e) entering any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (d);

(f) removing the computer or another thing from any place where it is situated for the purposes of doing the things mentioned in paragraph (c), and returning the computer or other thing to that place;

(g) if, having regard to other methods (if any) of doing the things mentioned in paragraph (c) which are likely to be as effective, it is reasonable in all the circumstances to do so:

(i) using any other computer or a communication in transit to do those things; and

(ii) if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;

(h) intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing mentioned in this subsection;

(i) any other thing reasonably incidental to any of the above;

at the following time:

Authorised Version C2025C00651 registered 28/11/2025

(j) at any time while the warrant is in force or within 28 days after it ceases to be in force;

(k) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (j)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).

(10) Subsection (9) does not authorise the doing of a thing that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer;

unless the doing of the thing is necessary to do one or more of the things specified in subsection (9); or

(b) cause any other material loss or damage to other persons lawfully using a computer, unless the loss or damage is reasonably necessary, and proportionate, to do one or more of the things specified in the warrant or authorised by subsection (9).

(11) If a computer or another thing is removed from a place in accordance with paragraph (9)(f), the computer or thing must be returned to the place as soon as is reasonably practicable to do so once the computer or thing is no longer required for the purposes of doing any thing mentioned in paragraph (9)(c).

Statutory conditions

(12) A data disruption warrant is subject to the following conditions:

(a) the warrant must not be executed in a manner that results in loss or damage to data unless the damage is reasonably necessary, and proportionate, to do one or more of the things specified in the warrant or authorised by subsection (9);

(b) the warrant must not be executed in a manner that causes a person to suffer a permanent loss of:

(i) money; or

(ii) digital currency; or

Authorised Version C2025C00651 registered 28/11/2025

(iii) property (other than data).

(13) Subsection (12) does not, by implication, limit the conditions to which a data disruption warrant may be subject.

(14) The conditions set out in subsection (12) must be specified in a data disruption warrant.

27KF Extension and variation of data disruption warrant

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

(a) for an extension of the warrant for a period of no more than 90 days after the day the warrant would otherwise expire; or

(b) for a variation of any of the other terms of the warrant.

(2) The application is to be made to an eligible Judge or to a nominated ART member and must be accompanied by the original warrant.

(3) Sections 27KA and 27KB apply, with any necessary changes, to an application under this section as if it were an application for the warrant.

(4) The eligible Judge or nominated ART member may grant an application if satisfied that the matters referred to in subsection 27KC(1) still exist, having regard to the matters in subsection 27KC(2).

(5) If the eligible Judge or nominated ART member grants the application, the eligible Judge or nominated ART member must endorse the new expiry date or the other varied term on the original warrant.

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

Authorised Version C2025C00651 registered 28/11/2025

27KG Revocation of data disruption warrant

(1) A data disruption warrant may, by instrument in writing, be revoked by an eligible Judge or nominated ART member on the initiative of the eligible Judge or nominated ART member at any time before the expiration of the period of validity specified in the warrant.

(2) If the circumstances set out in subsection 27KH(2) apply in relation to a data disruption warrant, the chief officer of the law enforcement agency to which the law enforcement officer to whom the warrant was issued belongs or is seconded must, by instrument in writing, revoke the warrant.

(3) The instrument revoking a warrant must be signed by the eligible Judge, the nominated ART member or the chief officer of the law enforcement agency, as the case requires.

(4) If an eligible Judge or nominated ART member revokes a warrant, the eligible Judge or nominated ART member must give a copy of the instrument of revocation to the chief officer of the law enforcement agency to which the law enforcement officer to whom the warrant was issued belongs or is seconded.

(5) If:

(a) an eligible Judge or nominated ART member revokes a warrant; and

(b) at the time of the revocation, a law enforcement officer is executing the warrant;

the law enforcement officer is not subject to any civil or criminal liability for any act done in the proper execution of that warrant before the officer is made aware of the revocation.

27KH Discontinuance of access and disruption under warrant

Scope

(1) This section applies if a data disruption warrant is issued.

Authorised Version C2025C00651 registered 28/11/2025

Discontinuance of access and disruption

(2) If:

(a) the data disruption warrant has been sought by or on behalf of a law enforcement officer; and

(b) the chief officer of the law enforcement agency to which the law enforcement officer belongs or is seconded is satisfied that access to, and disruption of, data under the warrant is no longer required for the purposes referred to in paragraph 27KA(1)(c);

the chief officer must, in addition to revoking the warrant under section 27KG, take the steps necessary to ensure that access to, and disruption of, data authorised by the warrant is discontinued.

(3) If the chief officer of a law enforcement agency is notified that a warrant has been revoked by an eligible Judge or a nominated ART member under section 27KG, the chief officer must take the steps necessary to ensure that access to, and disruption of, data authorised by the warrant is discontinued as soon as practicable.

(4) If the law enforcement officer to whom the warrant is issued, or who is primarily responsible for executing the warrant, believes that access to, and disruption of, data under the warrant is no longer necessary for the purposes referred to in paragraph 27KA(1)(c), the law enforcement officer must immediately inform the chief officer of the law enforcement agency to which the law enforcement officer belongs or is seconded.

27KJ Relationship of this Division to parliamentary privileges and immunities

To avoid doubt, this Division does not affect the law relating to the powers, privileges and immunities of any of the following:

(a) each House of the Parliament;

(b) the members of each House of the Parliament;

(c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

Authorised Version C2025C00651 registered 28/11/2025

Division 6—Network activity warrants

27KKA Sunsetting

This Division ceases to have effect 5 years after it commences.

27KK Application for network activity warrant

(1) The chief officer of the Australian Federal Police or the Australian Crime Commission may apply for the issue of a network activity warrant if the chief officer suspects on reasonable grounds that:

(a) a group of individuals is a criminal network of individuals; and

(b) access to data held in a computer (the ***target computer***) that is, from time to time, used, or likely to be used, by any of the individuals in the group will substantially assist in the collection of intelligence that:

(i) relates to the group or to any of the individuals in the group; and

(ii) is relevant to the prevention, detection or frustration of one or more kinds of relevant offences.

(2) For the purposes of subsection (1), it is immaterial whether:

(a) the identities of the individuals in the group can be ascertained; or

(b) the target computer can be identified; or

(c) the location of the target computer can be identified; or

(d) there are likely to be changes, from time to time, in the composition of the group.

Procedure for making applications

(3) An application under subsection (1) may be made to an eligible Judge or to a nominated ART member.

(4) An application:

Authorised Version C2025C00651 registered 28/11/2025

(a) must specify:
(i) the name of the applicant; and
(ii) the nature and duration of the warrant sought; and
(b) subject to this section, must be supported by an affidavit setting out the grounds on which the warrant is sought.

Unsworn applications

(5) If the chief officer of the Australian Federal Police or the Australian Crime Commission believes that:
(a) immediate access to data held in the target computer referred to in subsection (1) will substantially assist as described in paragraph (1)(b); and
(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made by the chief officer;

an application by the chief officer for a warrant under subsection (1) may be made before an affidavit is prepared or sworn.

(6) If subsection (5) applies, the applicant must:
(a) provide as much information as the eligible Judge or nominated ART member considers is reasonably practicable in the circumstances; and
(b) not later than 72 hours after the making of the application, send a duly sworn affidavit to the eligible Judge or nominated ART member, whether or not a warrant has been issued.

Target computer

(7) The target computer referred to in subsection (1):
(a) must be a computer that is, from time to time, used or likely to be used by an individual (whose identity may or may not be known); and
(b) may be one or more of the following:
(i) a particular computer;

Authorised Version C2025C00651 registered 28/11/2025

(ii) a computer that is, from time to time, on particular premises.

27KL Remote application

(1) If the chief officer of the Australian Federal Police or the Australian Crime Commission believes that it is impracticable for an application for a network activity warrant to be made in person, the application may be made under section 27KK 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 transmit a copy of the affidavit, whether sworn or unsworn, to the eligible Judge or to the nominated ART member who is to determine the application.

27KM Determining the application

(1) An eligible Judge or a nominated ART member may issue a network activity warrant if satisfied:

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

(aa) that the issue of the warrant is justified and proportionate, having regard to the kinds of offences in relation to which information will be obtained under the warrant; and

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

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

(2) In determining whether a network activity warrant should be issued, the eligible Judge or nominated ART member must have regard to:

(a) the nature and gravity of the conduct constituting the kinds of offences in relation to which information will be obtained under the warrant; and

Authorised Version C2025C00651 registered 28/11/2025

(b) the extent to which access to data under the warrant will assist in the collection of intelligence that:

(i) relates to the group referred to in paragraph 27KK(1)(a) or to any of the individuals in the group; and

(ii) is relevant to the prevention, detection or frustration of one or more kinds of relevant offences; and

(c) the likely intelligence value of any information sought to be obtained; and

(d) whether the things authorised by the warrant are proportionate to the likely intelligence value of any information sought to be obtained; and

(e) the existence of any alternative, or less intrusive, means of obtaining the information sought to be obtained; and

(f) the extent to which the execution of the warrant is likely to result in access to data of persons who are lawfully using a computer, and any privacy implications (to the extent known to the eligible Judge or nominated ART member) resulting from that access; and

(fa) if:

(i) the eligible Judge or nominated ART member believes on reasonable grounds that the data covered by the warrant (within the meaning of section 27KP) is data of a person who is working in a professional capacity as a journalist or of an employer of such a person; and

(ii) each of the offences referred to in paragraph 27KK(1)(b) is an offence against a secrecy provision;

whether the public interest in issuing the warrant outweighs:

(iii) the public interest in protecting the confidentiality of the identity of the journalist's source; and

(iv) the public interest in facilitating the exchange of information between journalists and members of the public so as to facilitate reporting of matters in the public interest; and

(g) any previous warrant sought or issued under this Division in relation to the group referred to in paragraph 27KK(1)(a).

Authorised Version C2025C00651 registered 28/11/2025

(2A) For the purposes of having regard to the nature and gravity of the conduct constituting the kinds of offences in relation to which information will be obtained under the warrant, the eligible Judge or nominated ART member must give weight to the following matters:

(a) whether that conduct amounts to:

(i) an activity against the security of the Commonwealth; or

(ii) an offence against Chapter 5 of the *Criminal Code*;

(b) whether that conduct amounts to:

(i) an activity against the proper administration of Government; or

(ii) an offence against Chapter 7 of the *Criminal Code*;

(c) whether that conduct:

(i) causes, or has the potential to cause, serious violence, or serious harm, to a person; or

(ii) amounts to an offence against Chapter 8 of the *Criminal Code*;

(d) whether that conduct:

(i) causes, or has the potential to cause, a danger to the community; or

(ii) amounts to an offence against Chapter 9 of the *Criminal Code*;

(e) whether that conduct:

(i) causes, or has the potential to cause, substantial damage to, or loss of, data, property or critical infrastructure; or

(ii) amounts to an offence against Chapter 10 of the *Criminal Code*;

(f) whether that conduct involves, or is related to, the commission of:

(i) transnational crime; or

(ii) serious crime; or

(iii) organised crime;

that is not covered by any of the preceding paragraphs.

Authorised Version C2025C00651 registered 28/11/2025

(2B) Subsection (2A) does not limit the matters that may be considered by the eligible Judge or nominated ART member.

(2C) To avoid doubt, this Act does not prevent a network activity warrant from being issued in a case where the conduct constituting the kinds of offences in relation to which information will be obtained under the warrant is not covered by subsection (2A).

(3) If a network activity warrant is issued in response to an application made by the chief officer of the Australian Federal Police or the Australian Crime Commission, the chief officer must:
  (a) notify the issue of the warrant to the Inspector-General of Intelligence and Security; and
  (b) do so within 7 days after the issue of the warrant.

(4) For the purposes of this section, ***secrecy provision*** means a provision of a law of the Commonwealth or of a State that prohibits:
  (a) the communication, divulging or publication of information; or
  (b) the production of, or the publication of the contents of, a document.

27KN What must a network activity warrant contain?

(1) A network activity warrant must:
  (a) state that the eligible Judge or nominated ART member issuing the warrant is satisfied of the matters referred to in subsection 27KM(1) and has had regard to the matters referred to in subsection 27KM(2); and
  (b) specify:
    (i) the name of the applicant; and
    (ii) the kinds of relevant offences in respect of which the warrant is issued; and
    (iii) the criminal network of individuals to which the warrant relates; and
    (iv) the date the warrant is issued; and

Authorised Version C2025C00651 registered 28/11/2025

(v) the period during which the warrant is in force (see subsection (2)); and

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

(vii) any conditions subject to which things may be done under the warrant; and

(c) if the warrant authorises the use of a surveillance device—specify:

(i) the surveillance device authorised to be used; and

(ii) the purpose or purposes for which the surveillance device may be used under the warrant.

(2) A warrant may only be issued for a period of no more than 90 days.

Note: The access to data held in the target computer pursuant to a warrant may be discontinued earlier—see section 27KS.

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

(4) For the purposes of subparagraph (1)(b)(iii), a criminal network of individuals may be specified by identifying one or more matters or things that are sufficient to identify the criminal network of individuals.

(5) As soon as practicable after completing and signing a warrant issued on a remote application, the person issuing it must:

(a) inform the applicant of:

(i) the terms of the warrant; and

(ii) the date on which, and the time at which, the warrant was issued; and

(b) give the warrant to the applicant while retaining a copy of the warrant for the person's own record.

Authorised Version C2025C00651 registered 28/11/2025

27KP What a network activity warrant authorises

(1) A network activity warrant must authorise the doing of specified things (subject to any restrictions or conditions specified in the warrant) in relation to the relevant target computer.

(2) The things that may be specified are any of the following that the eligible Judge or nominated ART member considers appropriate in the circumstances:

(a) entering specified premises for the purposes of doing the things mentioned in this subsection;

(b) entering any premises for the purposes of gaining entry to, or exiting, the specified premises;

(c) using:

(i) the target computer; or

(ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or

(iii) any other electronic equipment; or

(iv) a data storage device;

for the purpose of obtaining access to data (the ***relevant data***) that is held in the target computer at any time while the warrant is in force, in order to determine whether the relevant data is covered by the warrant;

(d) if necessary to achieve the purpose mentioned in paragraph (c)—adding, copying, deleting or altering other data in the target computer;

(e) if, having regard to other methods (if any) of obtaining access to the relevant data which are likely to be as effective, it is reasonable in all the circumstances to do so:

(i) using any other computer or a communication in transit to access the relevant data; and

(ii) if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;

(f) removing a computer or other thing from premises for the purposes of doing any thing specified in the warrant in

Authorised Version C2025C00651 registered 28/11/2025

accordance with this subsection, and returning the computer or other thing to the premises;

(g) copying any data to which access has been obtained, and that:

(i) appears to be relevant for the purposes of determining whether the relevant data is covered by the warrant; or

(ii) is covered by the warrant;

(h) intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing specified in the warrant in accordance with this subsection;

(i) using a surveillance device for the purposes of doing any thing specified in the warrant in accordance with this subsection;

(j) any other thing reasonably incidental to any of the above.

Note: As a result of the warrant, a person who, by means of a telecommunications facility, obtains access to data stored in a computer will not commit an offence under Part 10.7 of the *Criminal Code* or equivalent State or Territory laws (provided that the person acts within the authority of the warrant).

(3) If:

(a) a network activity warrant authorises the removal of a computer or other thing from premises as mentioned in paragraph (2)(f); and

(b) a computer or thing is removed from the premises in accordance with the warrant;

the computer or thing must be returned to the premises as soon as is reasonably practicable to do so once the computer or thing is no longer required for the purposes of doing any thing authorised by the warrant.

(4) For the purposes of paragraph (2)(g), if:

(a) access has been obtained to data; and

(b) the data is subject to a form of electronic protection;

the data is taken to be relevant for the purposes of determining whether the relevant data is covered by the warrant.

Authorised Version C2025C00651 registered 28/11/2025

When data is covered by a warrant

(5) For the purposes of this section, data is ***covered by*** a warrant if access to the data will substantially assist as described in paragraph 27KK(1)(b). To avoid doubt, it is immaterial whether the composition of the group mentioned in that paragraph changes during the period when the warrant is in force.

Certain acts not authorised

(6) Subsection (2) does not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer;

unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified in the warrant; or

(b) cause any other material loss or damage to other persons lawfully using a computer.

Warrant must provide for certain matters

(7) A network activity warrant must:

(a) authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant; and

(b) if the warrant authorises entering premises—state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.

Concealment of access etc.

(8) If any thing has been done in relation to a computer under:

(a) a network activity warrant; or

(b) this subsection;

then, in addition to the things specified in the warrant, the warrant authorises the doing of any of the following:

Authorised Version C2025C00651 registered 28/11/2025

(c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant or under this subsection;

(d) entering any premises where the computer is reasonably believed to be, for the purposes of doing the things mentioned in paragraph (c);

(e) entering any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (d);

(f) removing the computer or another thing from any place where it is situated for the purposes of doing the things mentioned in paragraph (c), and returning the computer or other thing to that place;

(g) if, having regard to other methods (if any) of doing the things mentioned in paragraph (c) which are likely to be as effective, it is reasonable in all the circumstances to do so:

(i) using any other computer or a communication in transit to do those things; and

(ii) if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;

(h) intercepting a communication passing over a telecommunications system, if the interception is for the purposes of doing any thing mentioned in this subsection;

(i) using a surveillance device, if the use is for the purposes of doing any thing mentioned in this subsection;

(j) any other thing reasonably incidental to any of the above;

at the following time:

(k) at any time while the warrant is in force or within 28 days after it ceases to be in force;

(l) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (k)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).

(9) Subsection (8) does not authorise the doing of a thing that is likely to:

Authorised Version C2025C00651 registered 28/11/2025

(a) materially interfere with, interrupt or obstruct:
(i) a communication in transit; or
(ii) the lawful use by other persons of a computer;
unless the doing of the thing is necessary to do one or more of the things specified in subsection (8); or
(b) cause any other material loss or damage to other persons lawfully using a computer.

(10) If a computer or another thing is removed from a place in accordance with paragraph (8)(f), the computer or thing must be returned to the place as soon as is reasonably practicable to do so once the computer or thing is no longer required for the purposes of doing any thing mentioned in paragraph (8)(c).

27KQ Extension and variation of network activity warrant

(1) If a network activity warrant was issued in response to an application by the chief officer of the Australian Federal Police or the Australian Crime Commission, the chief officer may apply, at any time before the expiry of the warrant:
(a) for an extension of the warrant for a period of no more than 90 days after the day the warrant would otherwise expire; or
(b) for a variation of any of the other terms of the warrant.

(2) The application is to be made to an eligible Judge or to a nominated ART member and must be accompanied by the original warrant.

(3) Sections 27KK and 27KL apply, with any necessary changes, to an application under this section as if it were an application for the warrant.

(4) The eligible Judge or nominated ART member may grant an application if satisfied that the matters referred to in subsection 27KM(1) still exist, having regard to the matters in subsection 27KM(2).

(5) If the eligible Judge or nominated ART member grants the application, the eligible Judge or nominated ART member must

Authorised Version C2025C00651 registered 28/11/2025

endorse the new expiry date or the other varied term on the original warrant.

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

(7) If a network activity warrant is extended or varied in response to an application made by the chief officer of the Australian Federal Police or the Australian Crime Commission, the chief officer must:

(a) notify the extension or variation to the Inspector-General of Intelligence and Security; and

(b) do so within 7 days after the extension or variation.

27KR Revocation of network activity warrant

(1) A network activity warrant may, by instrument in writing, be revoked by an eligible Judge or nominated ART member on the initiative of the eligible Judge or nominated ART member at any time before the expiration of the period of validity specified in the warrant.

(2) If the circumstances set out in subsection 27KS(2) apply in relation to a network activity warrant:

(a) if the warrant was issued in response to an application made by the chief officer of the Australian Federal Police—the chief officer of the Australian Federal Police must, by instrument in writing, revoke the warrant; or

(b) if the warrant was issued in response to an application made by the chief officer of the Australian Crime Commission—the chief officer of the Australian Crime Commission must, by instrument in writing, revoke the warrant.

(3) The instrument revoking a warrant must be signed by the eligible Judge, the nominated ART member, the chief officer of the Australian Federal Police or the chief officer of the Australian Crime Commission, as the case requires.

(4) If an eligible Judge or nominated ART member revokes a warrant, the eligible Judge or nominated ART member must give a copy of the instrument of revocation to:

Authorised Version C2025C00651 registered 28/11/2025

(a) if the warrant was issued in response to an application made by the chief officer of the Australian Federal Police—the chief officer of the Australian Federal Police; or

(b) if the warrant was issued in response to an application made by the chief officer of the Australian Crime Commission—the chief officer of the Australian Crime Commission.

(5) If:

(a) an eligible Judge or nominated ART member revokes a warrant; and

(b) at the time of the revocation, a law enforcement officer is executing the warrant;

the law enforcement officer is not subject to any civil or criminal liability for any act done in the proper execution of that warrant before the officer is made aware of the revocation.

(6) If:

(a) a network activity warrant was issued in response to an application made by the chief officer of the Australian Federal Police or the Australian Crime Commission; and

(b) an eligible Judge or nominated ART member revokes the warrant;

the chief officer must:

(c) notify the revocation to the Inspector-General of Intelligence and Security; and

(d) do so within 7 days after the revocation.

(7) If a network activity warrant is revoked by the chief officer of the Australian Federal Police or the Australian Crime Commission, the chief officer must:

(a) notify the revocation to the Inspector-General of Intelligence and Security; and

(b) do so within 7 days after the revocation.

Authorised Version C2025C00651 registered 28/11/2025

27KS Discontinuance of access under warrant

Scope

(1) This section applies if a network activity warrant is issued.

Discontinuance of access

(2) If:

(a) the warrant was sought by the chief officer of the Australian Federal Police or the Australian Crime Commission; and

(b) the chief officer is satisfied that access to data under the warrant is no longer required for the purpose referred to in paragraph 27KK(1)(b);

the chief officer must, in addition to revoking the warrant under section 27KR, take the steps necessary to ensure that access to data authorised by the warrant is discontinued.

(3) If:

(a) the warrant was sought by the chief officer of the Australian Federal Police or the Australian Crime Commission; and

(b) the chief officer is notified that the warrant has been revoked by an eligible Judge or a nominated ART member under section 27KR;

the chief officer must take the steps necessary to ensure that access to data authorised by the warrant is discontinued as soon as practicable.

(4) If the law enforcement officer who is primarily responsible for executing the warrant believes that access to data under the warrant is no longer necessary for the purpose referred to in paragraph 27KK(1)(b), the law enforcement officer must immediately inform the chief officer of the law enforcement agency to which the law enforcement officer belongs or is seconded.

Authorised Version C2025C00651 registered 28/11/2025

27KT Relationship of this Division to parliamentary privileges and immunities

To avoid doubt, this Division does not affect the law relating to the powers, privileges and immunities of any of the following:

(a) each House of the Parliament;

(b) the members of each House of the Parliament;

(c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

Authorised Version C2025C00651 registered 28/11/2025

Part 3—Emergency authorisations

27KU Sunsetting—emergency authorisation for disruption of data held in a computer

(1) Subsections 28(1C) and (1D) cease to have effect 5 years after they commence.

(2) An emergency authorisation for disruption of data held in a computer has no effect after the end of the 5-year period beginning at the commencement of this section.

28 Emergency authorisation—serious risks to person or property

(1) A law enforcement officer may apply to an appropriate authorising officer for an emergency authorisation for the use of a surveillance device if, in the course of an investigation of a relevant offence, the law enforcement officer reasonably suspects that:

(a) an imminent risk 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 risk; 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.

(1A) A law enforcement officer may apply to an appropriate authorising officer for an emergency authorisation for access to data held in a computer (the ***target computer***) if, in the course of an investigation of a relevant offence, the law enforcement officer reasonably suspects that:

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

Authorised Version C2025C00651 registered 28/11/2025

(b) access to data held in the target computer is immediately necessary for the purpose of dealing with that risk; and

(c) the circumstances are so serious and the matter is of such urgency that access to data held in the target computer is warranted; and

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

(1B) The target computer mentioned in subsection (1A) may be any one or more of the following:

(a) a particular computer;

(b) a computer on particular premises;

(c) a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).

(1C) A law enforcement officer of the Australian Federal Police or the Australian Crime Commission may apply to an appropriate authorising officer for an emergency authorisation for disruption of data held in a computer (the ***target computer***) if, in the course of an investigation of a relevant offence, the law enforcement officer reasonably suspects that:

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

(b) disruption of data held in the target computer is immediately necessary for the purpose of dealing with that risk; and

(ba) there are no alternative methods that:

(i) could have been used by law enforcement officers to help reduce or avoid that risk; and

(ii) are likely to be as effective as disruption of data held in the target computer; and

(c) the circumstances are so serious and the matter is of such urgency that disruption of data held in the target computer is warranted; and

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

Authorised Version C2025C00651 registered 28/11/2025

(1D) The target computer mentioned in subsection (1C) may be any one or more of the following:

(a) a particular computer;

(b) a computer on particular premises;

(c) a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).

(2) If the application mentioned in subsection (1) or (1A) is being made by or on behalf of a State or Territory law enforcement officer, the reference in that subsection to a relevant offence does not include a reference to a State offence that has a federal aspect.

(3) The application mentioned in subsection (1), (1A) or (1C) may be made orally, in writing or by telephone, fax, email or any other means of communication.

(4) The appropriate authorising officer may give the emergency authorisation if satisfied that there are reasonable grounds for the suspicion founding the application mentioned in subsection (1), (1A) or (1C).

(4A) In deciding whether to give an emergency authorisation for disruption of data held in a computer, the appropriate authorising officer must have regard to:

(a) the extent to which the execution of the emergency authorisation is likely to result in access to, or disruption of, data of persons lawfully using a computer; and

(b) whether the likely impact of the execution of the emergency authorisation on persons lawfully using a computer is proportionate, having regard to the risk of serious violence or substantial damage referred to in paragraph (1C)(a).

(4B) Subsection (4A) does not limit the matters to which the appropriate authorising officer may have regard.

Statutory conditions—disruption of data held in a computer

(5) An emergency authorisation for disruption of data held in a computer is subject to the following conditions:

Authorised Version C2025C00651 registered 28/11/2025

(a) the authorisation must not be executed in a manner that results in damage to data unless the damage is reasonably necessary and proportionate, having regard to the risk of serious violence or substantial damage referred to in paragraph (1C)(a);

(b) the authorisation must not be executed in a manner that causes a person to suffer a permanent loss of:

(i) money; or

(ii) digital currency; or

(iii) property (other than data).

29 Emergency authorisation—urgent circumstances relating to recovery order

(1) A law enforcement officer may apply to an appropriate authorising officer for an emergency authorisation for the use of a surveillance device if:

(a) a recovery order is in force; and

(b) the law enforcement officer reasonably suspects that:

(i) the circumstances are so urgent as to warrant the immediate use of a surveillance device; and

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

(1A) A law enforcement officer may apply to an appropriate authorising officer for an emergency authorisation for access to data held in a computer (the ***target computer***) if:

(a) a recovery order is in force; and

(b) the law enforcement officer reasonably suspects that:

(i) the circumstances are so urgent as to warrant immediate access to data held in the target computer; and

(ii) it is not practicable in the circumstances to apply for a computer access warrant.

(1B) The target computer may be any one or more of the following:

(a) a particular computer;

Authorised Version C2025C00651 registered 28/11/2025

(b) a computer on particular premises;

(c) a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).

(2) The application mentioned in subsection (1) or (1A) may be made orally, in writing or by telephone, fax, email or any other means of communication.

(3) The appropriate authorising officer may give the emergency authorisation if satisfied that the recovery order is in force and that there are reasonable grounds for the suspicion founding the application mentioned in subsection (1) or (1A).

30 Emergency authorisation—risk of loss of evidence

(1) If:

(a) a law enforcement officer is conducting an investigation into:

(ii) an offence against section 233BAA of the *Customs Act 1901* (with respect to goods listed in Schedule 4 to the *Customs (Prohibited Imports) Regulations 1956* or in Schedule 8 or 9 to the *Customs (Prohibited Exports) Regulations 1958*); or

(iv) an offence under the *Crimes (Traffic in Narcotic Drugs and Psychotropic Substances) Act 1990* or an offence against Part 9.1 of the *Criminal Code* (other than section 308.1 or 308.2); or

(vi) an offence against section 73.2 or 73.3 of the *Criminal Code*; or

(vii) an offence against Division 91 of the *Criminal Code* (espionage); or

(viii) an offence under Subdivision A of Division 72 or Division 80, 101, 102, 103, 111, 112, 113, 270, 272, 273 or 273A of the *Criminal Code*; or

(ix) an offence against section 233B or 233C of the *Migration Act 1958*;

or more than one offence; and

(b) the law enforcement officer reasonably suspects that:

Authorised Version C2025C00651 registered 28/11/2025

(i) the use of the surveillance device is immediately necessary to prevent the loss of any evidence relevant to that investigation; and

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

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

the law enforcement officer may apply to an appropriate authorising officer for an emergency authorisation for the use of a surveillance device.

(1A) If:

(a) a law enforcement officer is conducting an investigation into:

(i) an offence against section 233BAA of the *Customs Act 1901* (with respect to goods listed in Schedule 4 to the *Customs (Prohibited Imports) Regulations 1956* or in Schedule 8 or 9 to the *Customs (Prohibited Exports) Regulations 1958*); or

(ii) an offence under the *Crimes (Traffic in Narcotic Drugs and Psychotropic Substances) Act 1990* or an offence against Part 9.1 of the *Criminal Code* (other than section 308.1 or 308.2); or

(iii) an offence against section 73.2 or 73.3 or Division 91 of the *Criminal Code*; or

(iv) an offence under Subdivision A of Division 72 or Division 80, 101, 102, 103, 111, 112, 113, 270, 272, 273 or 273A of the *Criminal Code*; or

(v) an offence against section 233B or 233C of the *Migration Act 1958*;

or more than one offence; and

(b) the law enforcement officer reasonably suspects that:

(i) access to data held in a computer (the ***target computer***) is immediately necessary to prevent the loss of any evidence relevant to that investigation; and

Authorised Version C2025C00651 registered 28/11/2025

(ii) the circumstances are so serious and the matter is of such urgency that access to data held in the target computer is warranted; and

(iii) it is not practicable in the circumstances to apply for a computer access warrant;

the law enforcement officer may apply to an appropriate authorising officer for an emergency authorisation for access to data held in the target computer.

(1B) The target computer may be any one or more of the following:

(a) a particular computer;

(b) a computer on particular premises;

(c) a computer associated with, used by or likely to be used by, a person (whose identity may or may not be known).

(2) The application mentioned in subsection (1) or (1A) may be made orally, in writing or by telephone, fax, email or any other means of communication.

(3) In the case of an application mentioned in subsection (1), the appropriate authorising officer may give the emergency authorisation if satisfied that:

(a) an investigation is being conducted into an offence referred to in paragraph (1)(a); and

(b) there are reasonable grounds for the suspicion referred to in paragraph (1)(b).

(4) In the case of an application mentioned in subsection (1A), the appropriate authorising officer may give the emergency authorisation if satisfied that:

(a) an investigation is being conducted into an offence referred to in paragraph (1A)(a); and

(b) there are reasonable grounds for the suspicion referred to in paragraph (1A)(b).

Authorised Version C2025C00651 registered 28/11/2025

31 Record of emergency authorisations to be made

(1) As soon as practicable after an appropriate authorising officer gives an emergency authorisation, the officer must make a written record of the giving of that authorisation, including in the record:

(a) the name of the applicant for the authorisation; and

(b) the date and time the authorisation was given; and

(c) the nature of the authorisation given.

(2) A written record made under subsection (1) is not a legislative instrument.

32 Attributes of emergency authorisations

(1) An emergency authorisation for the use of a surveillance device may authorise the law enforcement officer to whom it is given:

(a) to use more than one kind of surveillance device; and

(b) to use more than one surveillance device of any particular kind.

(2) An emergency authorisation for the use of a surveillance device may authorise anything that a surveillance device warrant may authorise.

(2A) An emergency authorisation for access to data held in a computer may authorise anything that a computer access warrant may authorise.

(2B) An emergency authorisation for disruption of data held in a computer may authorise anything that a data disruption warrant may authorise.

(3) A law enforcement officer may use a surveillance device under an emergency authorisation only if he or she is acting in the performance of his or her duty.

(3A) A law enforcement officer may, under an emergency authorisation, access data held in a computer only if the officer is acting in the performance of the officer's duty.

Authorised Version C2025C00651 registered 28/11/2025

(3B) A law enforcement officer may, under an emergency authorisation, disrupt data held in a computer only if the officer is acting in the performance of the officer's duty.

(4) Nothing in this Part (other than subsection (2A) or (2B) of this section) authorises the doing of anything for which a warrant would be required under the *Telecommunications (Interception and Access) Act 1979*.

33 Application for approval of emergency authorisation

(1) Within 48 hours after giving an emergency authorisation to a law enforcement officer, the appropriate authorising officer who gave the authorisation (or another person on that appropriate authorising officer's behalf) must apply, for approval of the giving of the emergency authorisation, to:

(a) for an authorisation given to a law enforcement officer of the National Anti-Corruption Commission—an eligible Judge; or

(b) otherwise—an eligible Judge or a nominated ART member.

(2) In the case of an application for an emergency authorisation for the use of a surveillance device, the application:

(a) must specify:

(i) the name of the applicant for the approval; and

(ii) the kind or kinds of surveillance device to which the emergency authorisation relates 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; and

(c) must be accompanied by a copy of the written record made under section 31 in relation to the emergency authorisation.

(2A) In the case of an application for an emergency authorisation for access to data held in a computer, the application:

(a) must specify:

(i) the name of the applicant for the approval; and

Authorised Version C2025C00651 registered 28/11/2025

(ii) 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; and

(c) must be accompanied by a copy of the written record made under section 31 in relation to the emergency authorisation.

(2B) In the case of an application for an emergency authorisation for disruption of data held in a computer, the application:

(a) must specify:

(i) the name of the applicant for the approval; and

(ii) 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; and

(c) must be accompanied by a copy of the written record made under section 31 in relation to the emergency authorisation.

(3) The eligible Judge or nominated ART member may refuse to consider the application until the applicant gives the Judge or member all the information the Judge or member requires about the application in the way the Judge or member requires.

(4) An application for approval of the giving of an emergency authorisation and any instrument in support of such an application is not a legislative instrument.

34 Consideration of application

(1) Before deciding an application for approval of the giving of an emergency authorisation given under subsection 28(1), the eligible Judge or nominated ART member considering the application 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;

Authorised Version C2025C00651 registered 28/11/2025

(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.

(1A) Before deciding an application for approval of the giving of an emergency authorisation given in response to an application under subsection 28(1A), the eligible Judge or nominated ART member considering the application must, in particular, and being mindful of the intrusive nature of accessing data held in the target computer mentioned in that subsection, 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 computer access 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 computer access warrant.

(1B) Before deciding an application for approval of the giving of an emergency authorisation given in response to an application under subsection 28(1C), the eligible Judge or nominated ART member considering the application must, in particular, and being mindful of the intrusive nature of accessing and disrupting data held in the

Authorised Version C2025C00651 registered 28/11/2025

target computer mentioned in that subsection, 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 data disruption warrant would have helped reduce or avoid the risk;

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

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

(e) how much the use of alternative methods 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 data disruption warrant.

(2) Before deciding an application for approval of the giving of an emergency authorisation given under subsection 29(1), the eligible Judge or nominated ART member considering the application must, in particular, and being mindful of the intrusive nature of using a surveillance device, consider the following:

(a) the urgency of enforcing the recovery order;

(b) the extent to which use of a surveillance device would assist in the location and safe recovery of the child to whom the recovery order relates;

(c) the extent to which law enforcement officers could have used alternative methods to assist in the location and safe recovery of the child;

(d) how much the use of alternative methods to assist in the location and safe recovery of the child might have prejudiced the effective enforcement of the recovery order;

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

(2A) Before deciding an application for approval of the giving of an emergency authorisation given in response to an application under subsection 29(1A), the eligible Judge or nominated ART member

Authorised Version C2025C00651 registered 28/11/2025

considering the application must, in particular, and being mindful of the intrusive nature of accessing data held in the target computer mentioned in that subsection, consider the following:

(a) the urgency of enforcing the recovery order;

(b) the extent to which access to data held in the target computer mentioned in that subsection would assist in the location and safe recovery of the child to whom the recovery order relates;

(c) the extent to which law enforcement officers could have used alternative methods to assist in the location and safe recovery of the child;

(d) how much the use of alternative methods to assist in the location and safe recovery of the child might have prejudiced the effective enforcement of the recovery order;

(e) whether or not it was practicable in the circumstances to apply for a computer access warrant.

(3) Before deciding an application for approval of the giving of an emergency authorisation given under subsection 30(1), the eligible Judge or nominated ART member 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 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) whether or not it was practicable in the circumstances to apply for a surveillance device warrant.

(4) Before deciding an application for approval of the giving of an emergency authorisation given in response to an application under subsection 30(1A), the eligible Judge or nominated ART member must, in particular, and being mindful of the intrusive nature of

Authorised Version C2025C00651 registered 28/11/2025

accessing data held in the target computer mentioned in that subsection, consider the following:

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

(b) the extent to which issuing a computer access 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) whether or not it was practicable in the circumstances to apply for a computer access warrant.

35 Judge or nominated ART member may approve giving of an emergency authorisation for the use of a surveillance device

(1) After considering an application for approval of the giving of an emergency authorisation in response to an application under subsection 28(1), the eligible Judge or nominated ART member may give the approval if satisfied that there were reasonable grounds to suspect 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 of the giving of an emergency authorisation in response to an application under subsection 29(1) in relation to a recovery order, the eligible Judge or nominated ART member may give the approval if satisfied that:

(a) the recovery order was in force at the time the emergency authorisation was given; and

(b) there were reasonable grounds to suspect that:

Authorised Version C2025C00651 registered 28/11/2025

(i) the enforcement of the recovery order was urgent; and

(ii) using a surveillance device may have assisted in the prompt location and safe recovery of the child to whom the order relates; and

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

(3) After considering an application for approval of the giving of an emergency authorisation in response to an application under subsection 30(1), the eligible Judge or nominated ART member may give the approval if satisfied that:

(a) there were reasonable grounds to suspect that:

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

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

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

(4) If, under subsection (1), (2) or (3), the eligible Judge or nominated ART member approves the giving of an emergency authorisation, the Judge or member may:

(a) unless paragraph (b) applies—issue a surveillance device warrant for the continued use of the surveillance device as if the application for the approval were an application for a surveillance device warrant under Division 2 of Part 2; or

(b) if the Judge or member is satisfied that since the application for the emergency authorisation the activity that required surveillance has ceased—order that the use of the surveillance device cease.

(5) If, under subsection (1), (2) or (3), the eligible Judge or nominated ART member does not approve the giving of an emergency authorisation, the Judge or member may:

(a) order that the use of the surveillance device cease; or

(b) if the Judge or member is of the view that although the situation did not warrant the emergency authorisation at the time that authorisation was given, the use of a surveillance

Authorised Version C2025C00651 registered 28/11/2025

device warrant under Division 2 of Part 2 is currently justified—issue a surveillance device warrant for the subsequent use of such a device as if the application for the approval were an application for a surveillance device warrant under Division 2 of Part 2.

(6) In any case, the eligible Judge or nominated ART member 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 a manner specified in the order, not being a manner that involves the destruction of that information.

35A Judge or nominated ART member may approve giving of an emergency authorisation for access to data held in a computer

(1) After considering an application for approval of the giving of an emergency authorisation in response to an application under subsection 28(1A), the eligible Judge or nominated ART member may give the approval if satisfied that there were reasonable grounds to suspect that:

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

(b) accessing data held in the target computer mentioned in that subsection may have helped reduce the risk; and

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

(2) After considering an application for approval of the giving of an emergency authorisation in response to an application under subsection 29(1A) in relation to a recovery order, the eligible Judge or nominated ART member may give the approval if satisfied that:

(a) the recovery order was in force at the time the emergency authorisation was given; and

(b) there were reasonable grounds to suspect that:

(i) the enforcement of the recovery order was urgent; and

Authorised Version C2025C00651 registered 28/11/2025

(ii) accessing data held in the target computer mentioned in that subsection may have assisted in the prompt location and safe recovery of the child to whom the order relates; and

(iii) it was not practicable in the circumstances to apply for a computer access warrant.

(3) After considering an application for approval of the giving of an emergency authorisation in response to an application under subsection 30(1A), the eligible Judge or nominated ART member may give the approval if satisfied that:

(a) there were reasonable grounds to suspect that:

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

(ii) accessing data held in the target computer mentioned in that subsection may have helped reduce the risk; and

(b) it was not practicable in the circumstances to apply for a computer access warrant.

(4) If, under subsection (1), (2) or (3), the eligible Judge or nominated ART member approves the giving of an emergency authorisation, the eligible Judge or nominated ART member may:

(a) unless paragraph (b) applies—issue a computer access warrant relating to the continued access to data held in the relevant target computer as if the application for the approval were an application for a computer access warrant under Division 4 of Part 2; or

(b) if the eligible Judge or nominated ART member is satisfied that, since the application for the emergency authorisation, the activity that required access to data held in the relevant target computer has ceased—order that access to data held in that computer cease.

(5) If, under subsection (1), (2) or (3), the eligible Judge or nominated ART member does not approve the giving of an emergency authorisation, the eligible Judge or nominated ART member may:

(a) order that access to data held in the relevant target computer cease; or

Authorised Version C2025C00651 registered 28/11/2025

(b) if the eligible Judge or nominated ART member is of the view that, although the situation did not warrant the emergency authorisation at the time that authorisation was given, the use of a computer access warrant under Division 4 of Part 2 is currently justified—issue a computer access warrant relating to the subsequent access to such data as if the application for the approval were an application for a computer access warrant under Division 4 of Part 2.

(6) In any case, the eligible Judge or nominated ART member 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 a manner specified in the order, so long as the manner does not involve the destruction of that information.

35B Judge or nominated ART member may approve giving of an emergency authorisation for disruption of data held in a computer

(1) After considering an application for approval of the giving of an emergency authorisation in response to an application under subsection 28(1C), the eligible Judge or nominated ART member may give the approval if satisfied that there were reasonable grounds to suspect that:

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

(b) disruption of data held in the target computer mentioned in that subsection may have helped reduce the risk; and

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

(2) If, under subsection (1), the eligible Judge or nominated ART member approves the giving of an emergency authorisation, the eligible Judge or nominated ART member may:

(a) unless paragraph (b) applies—issue a data disruption warrant relating to the continued access to, and disruption of, data held in the relevant target computer as if the application for

Authorised Version C2025C00651 registered 28/11/2025

the approval were an application for a data disruption warrant under Division 5 of Part 2; or

(b) if the eligible Judge or nominated ART member is satisfied that, since the application for the emergency authorisation, the activity that required access to, and disruption of, data held in the relevant target computer has ceased—order that access to, and disruption of, data held in that computer cease.

(3) If, under subsection (1), the eligible Judge or nominated ART member does not approve the giving of an emergency authorisation, the eligible Judge or nominated ART member may:

(a) order that access to, and disruption of, data held in the relevant target computer cease; or

(b) if the eligible Judge or nominated ART member is of the view that, although the situation did not warrant the emergency authorisation at the time that authorisation was given, the use of a data disruption warrant under Division 5 of Part 2 is currently justified—issue a data disruption warrant relating to the subsequent access to, and disruption of, such data as if the application for the approval were an application for a data disruption warrant under Division 5 of Part 2.

(4) In any case, the eligible Judge or nominated ART member 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 a manner specified in the order, so long as the manner does not involve the destruction of that information.

36 Admissibility of evidence

If the giving of an emergency authorisation is approved under section 35, 35A or 35B, any evidence obtained because of the exercise of powers under that authorisation is not inadmissible in any proceeding only because the evidence was obtained before the approval.

Authorised Version C2025C00651 registered 28/11/2025

36A Relationship of this Part to parliamentary privileges and immunities

To avoid doubt, this Part does not affect the law relating to the powers, privileges and immunities of any of the following:

(a) each House of the Parliament;

(b) the members of each House of the Parliament;

(c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

Authorised Version C2025C00651 registered 28/11/2025

Part 4—Use of certain surveillance devices without warrant

37 Use of optical surveillance devices without warrant

(1) A federal law enforcement officer acting in the course of his or her duties may, without warrant, use an optical surveillance device for any purpose:

(a) if the officer belongs or is seconded to the Australian Federal Police—that is within the functions of the Australian Federal Police set out in section 8 of the *Australian Federal Police Act 1979*; or

(aa) if the officer belongs or is seconded to the National Anti-Corruption Commission—that is within the functions of the National Anti-Corruption Commissioner set out in section 17 of the *National Anti-Corruption Commission Act 2022*; or

(b) if the officer belongs or is seconded to the Australian Crime Commission—that is within the functions of the Commission set out in section 7A of the *Australian Crime Commission Act 2002*;

if the use of that device does not involve:

(c) entry onto premises without permission; or

(d) interference without permission with any vehicle or thing.

(2) A State or Territory law enforcement officer acting in the course of his or her duties may, without warrant, use an optical surveillance device in the investigation of a relevant offence (other than a State offence that has a federal aspect) if the use of that device does not involve:

(a) entry onto premises without permission; or

(b) interference without permission with any vehicle or thing.

(3) A State or Territory law enforcement officer acting in the course of his or her duties may, without warrant, use an optical surveillance

Authorised Version C2025C00651 registered 28/11/2025

device in the location and safe recovery of a child to whom a recovery order relates if the use of that device does not involve:

(a) a trespass on premises; or

(b) interference without permission with any vehicle or thing.

(4) If a Part 5.3 supervisory order is in force in relation to a person, a State or Territory law enforcement officer acting in the course of his or her duties may, without warrant, use an optical surveillance device to obtain information about the activities of the person for either of the following purposes:

(a) achieving a Part 5.3 object;

(b) determining whether the Part 5.3 supervisory order has been, or is being, complied with;

if the use of that device does not involve:

(e) entry onto premises without permission; or

(f) interference without permission with any vehicle or thing.

(5) If a community safety supervision order is in force in relation to a person, a State or Territory law enforcement officer acting in the course of the officer's duties may, without warrant, use an optical surveillance device to obtain information about the activities of the person for either of the following purposes:

(a) achieving a Part 9.10 object;

(b) determining whether the community safety supervision order has been, or is being, complied with;

if the use of that device does not involve:

(c) entry onto premises without permission; or

(d) interference without permission with any vehicle or thing.

38 Use of surveillance devices without warrant for listening to or recording words in limited circumstances

(1) A federal law enforcement officer acting in the course of his or her duties may, without warrant, use a surveillance device for any purpose involving listening to, or recording, words spoken by a person:

Authorised Version C2025C00651 registered 28/11/2025

(a) if the officer belongs or is seconded to the Australian Federal Police—that is within the functions of the Australian Federal Police set out in section 8 of the *Australian Federal Police Act 1979*; or

(aa) if the officer belongs or is seconded to the National Anti-Corruption Commission—that is within the functions of the National Anti-Corruption Commissioner set out in section 17 of the *National Anti-Corruption Commission Act 2022*; or

(b) if the officer belongs or is seconded to the Australian Crime Commission—that is within the functions of the Commission set out in section 7A of the *Australian Crime Commission Act 2002*;

if the use of that device for that listening or recording purpose is confined to circumstances where:

(c) the law enforcement officer is the speaker of the words or is a person, or is included in a class or group of persons, by whom the speaker of the words intends, or should reasonably expect, the words to be heard; or

(d) the law enforcement officer listens to or records the words with the consent, express or implied, of a person who is permitted to listen to or record the words by paragraph (c) or by subsection (4).

(2) A State or Territory law enforcement officer acting in the course of his or her duties and in the investigation of a relevant offence (other than a State offence that has a federal aspect) may, without warrant, use a surveillance device for any purpose involving listening to, or recording, words spoken by a person if the use of that device for that listening or recording purpose is confined to circumstances where:

(a) the State or Territory law enforcement officer is the speaker of the words or is a person, or is included in a class or group of persons, by whom the speaker of the words intends, or should reasonably expect, the words to be heard; or

Authorised Version C2025C00651 registered 28/11/2025

(b) the State or Territory law enforcement officer listens to or records the words with the consent, express or implied, of a person who is permitted to listen to or record the words:

(i) by paragraph (a); or

(ii) so far as subsection (5) applies in relation to that investigation—by that subsection.

(3) A State or Territory law enforcement officer acting in the course of his or her duties and in relation to the location and safe recovery of a child to whom a recovery order relates may, without warrant, use a surveillance device for any purpose involving listening to, or recording, words spoken by a person if the use of that device for that listening or recording purpose is confined to circumstances where:

(a) the State or Territory law enforcement officer is the speaker of the words or is a person, or is included in a class or group of persons, by whom the speaker of the words intends, or should reasonably expect, the words to be heard; or

(b) the State or Territory law enforcement officer listens to or records the words with the consent, express or implied, of a person who is permitted to listen to or record the words:

(i) by paragraph (a); or

(ii) so far as subsection (5) applies in relation to the location and safe recovery of the child—by that subsection.

(3A) If a Part 5.3 supervisory order is in force in relation to a person, a State or Territory law enforcement officer acting in the course of his or her duties may, without warrant, use a surveillance device to obtain information relating to the person for either of the following purposes:

(a) achieving a Part 5.3 object;

(b) determining whether the Part 5.3 supervisory order has been, or is being, complied with;

if the use involves listening to, or recording, words spoken by a person, and the use is confined to circumstances where:

(e) the State or Territory law enforcement officer is the speaker of the words or is a person, or is included in a class or group

Authorised Version C2025C00651 registered 28/11/2025

of persons, by whom the speaker of the words intends, or should reasonably expect, the words to be heard; or

(f) the State or Territory law enforcement officer listens to or records the words with the consent, express or implied, of a person who is permitted to listen to or record the words:

(i) by paragraph (e); or

(ii) so far as subsection (6) applies in relation to the Part 5.3 supervisory order—by that subsection.

(3B) If a community safety supervision order is in force in relation to a person, a State or Territory law enforcement officer acting in the course of the officer's duties may, without warrant, use a surveillance device to obtain information relating to the person for either of the following purposes:

(a) achieving a Part 9.10 object;

(b) determining whether the community safety supervision order has been, or is being, complied with;

if the use involves listening to, or recording, words spoken by a person, and the use is confined to circumstances where:

(c) the State or Territory law enforcement officer is the speaker of the words or is a person, or is included in a class or group of persons, by whom the speaker of the words intends, or should reasonably expect, the words to be heard; or

(d) the State or Territory law enforcement officer listens to or records the words with the consent, express or implied, of a person who is permitted to listen to or record the words:

(i) by paragraph (c); or

(ii) so far as subsection (7) applies in relation to the community safety supervision order—by that subsection.

(4) A person (other than a federal law enforcement officer) who is assisting a federal law enforcement officer acting in the course of his or her duties may, without warrant, use a surveillance device for any purpose:

(a) that involves listening to, or recording, words spoken by a person; and

Authorised Version C2025C00651 registered 28/11/2025

(b) that is referred to in subsection (1);

if the first-mentioned person is the speaker of the words or is a person, or is included in a class or group of persons, by whom the speaker of the words intends, or should reasonably expect, the words to be heard.

(5) A person (other than a State or Territory law enforcement officer) who is assisting a State or Territory law enforcement officer who is acting in the course of his or her duties in relation to:

(a) the investigation of a relevant offence (other than a State offence that has a federal aspect); or

(b) the location and safe recovery of a child to whom a recovery order relates;

may, without warrant, use a surveillance device for any purpose that involves listening to, or recording, words spoken by a person if the first-mentioned person is the speaker of the words or is a person, or is included in a class or group of persons, by whom the speaker of the words intends, or should reasonably expect, the words to be heard.

(6) If:

(a) a Part 5.3 supervisory order is in force in relation to a person; and

(b) a person (other than a State or Territory law enforcement officer) is assisting a State or Territory law enforcement officer who is acting in the course of his or her duties in relation to either of the following purposes:

(i) achieving a Part 5.3 object;

(ii) determining whether the Part 5.3 supervisory order has been, or is being, complied with;

the person assisting may, without warrant, use a surveillance device to obtain information relating to the person mentioned in paragraph (a) if:

(c) the use involves listening to, or recording, words spoken by a person; and

(d) the person assisting is the speaker of the words or is a person, or is included in a class or group of persons, by whom the

Authorised Version C2025C00651 registered 28/11/2025

speaker of the words intends, or should reasonably expect, the words to be heard.

(7) If:

(a) a community safety supervision order is in force in relation to a person; and

(b) a person (other than a State or Territory law enforcement officer) is assisting a State or Territory law enforcement officer who is acting in the course of the officer's duties in relation to either of the following purposes:

(i) achieving a Part 9.10 object;

(ii) determining whether the community safety supervision order has been, or is being, complied with;

the person assisting may, without warrant, use a surveillance device to obtain information relating to the person mentioned in paragraph (a) if:

(c) the use involves listening to, or recording, words spoken by a person; and

(d) the person assisting is the speaker of the words or is a person, or is included in a class or group of persons, by whom the speaker of the words intends, or should reasonably expect, the words to be heard.

39 Use and retrieval of tracking devices without warrant in certain circumstances

(1) A law enforcement officer may, with the written permission of an appropriate authorising officer, use a tracking device without a warrant in the investigation of a relevant offence.

(2) If the law enforcement officer referred to in subsection (1) is a State or Territory law enforcement officer, the reference in subsection (1) to a relevant offence does not include a reference to a State offence that has a federal aspect.

(3) A law enforcement officer may, with the written permission of an appropriate authorising officer, use a tracking device without a

Authorised Version C2025C00651 registered 28/11/2025

warrant in the location and safe recovery of a child to whom a recovery order relates.

(3A) A federal law enforcement officer may, with the written permission of an appropriate authorising officer, use a tracking device without a warrant for the purposes of an integrity operation.

(3B) If a Part 5.3 supervisory order is in force in relation to a person, a law enforcement officer may, with the written permission of an appropriate authorising officer, use a tracking device without a warrant to obtain information relating to the person for either of the following purposes:

(a) achieving a Part 5.3 object;

(b) determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with.

(3C) If a community safety supervision order is in force in relation to a person, a law enforcement officer may, with the written permission of an appropriate authorising officer, use a tracking device without a warrant to obtain information relating to the person for either of the following purposes:

(a) achieving a Part 9.10 object;

(b) determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with.

(4) Subsections (1), (3), (3A), (3B) and (3C) have effect despite any other law of the Commonwealth or of a State or self-governing Territory (including any principle of the common law) forbidding the use of such a device without a warrant.

(5) A tracking device authorisation given under subsection (1), (3), (3A), (3B) or (3C) may authorise the law enforcement officer to use more than one tracking device.

(6) If an appropriate authorising officer gives a tracking device authorisation under this section, an appropriate authorising officer

Authorised Version C2025C00651 registered 28/11/2025

may also authorise the retrieval, without a warrant, of a tracking device to which the tracking device authorisation relates.

(7) A tracking device authorisation given under subsection (1), (3), (3A), (3B) or (3C) and an authorisation for the retrieval of a tracking device given under subsection (6) must indicate the period, not exceeding 90 days, for which the authorisation remains in force.

(8) An appropriate authorising officer must not give permission under this section for the use, installation or retrieval of a tracking device if the installation of the device, or its retrieval, involves entry onto premises without permission or an interference with the interior of a vehicle without permission.

Note: Section 22 deals with applications for a retrieval warrant in respect of a tracking device that was lawfully installed under a tracking device authorisation.

(9) For the purposes of obtaining the permission of an appropriate authorising officer, the law enforcement officer wishing to use that device:

(a) must apply, orally or in writing, to the appropriate authorising officer; and

(b) must address, in that application, the matters that would be required to be addressed if the law enforcement officer were making an application for a surveillance device warrant or a retrieval warrant, as the case requires.

(10) Subsection 18(1), subparagraphs 18(2)(a)(i), 18(2)(b)(i) and 18(2)(c)(i), paragraphs 18(3)(a), (b) and (g) and subsections 18(4), (6) and (7) apply in relation to a tracking device authorisation authorising the use of a tracking device as if:

(a) references in those provisions to a surveillance device warrant were references to a tracking device authorisation authorising the use of a tracking device; and

(b) references in those provisions to a surveillance device were references to a tracking device.

Authorised Version C2025C00651 registered 28/11/2025

(11) Paragraphs 26(1)(a), (c), (d) and (e) and subsections 26(2) and (3) apply in relation to a tracking device authorisation authorising the retrieval of a tracking device as if:

(a) references in those provisions to a retrieval warrant were references to a tracking device authorisation authorising the retrieval of a tracking device; and

(b) references in those provisions to a surveillance device were references to a tracking device.

(12) A law enforcement officer may use a tracking device authorisation only if he or she is acting in the performance of his or her duty.

40 Record of tracking device authorisations to be kept

(1) As soon as practicable after an appropriate authorising officer gives a tracking device authorisation, the officer must make a written record of the giving of that authorisation, including in the record:

(a) the name of the applicant for the authorisation; and

(b) the date and time the authorisation was given; and

(c) if the authorisation authorises the use of a tracking device in relation to the investigation of an alleged relevant offence or offences—the alleged offence or offences in respect of which the authorisation is given; and

(d) if the authorisation authorises the use of a tracking device in relation to a recovery order—the date the order was made and the name of the child to whom the order relates; and

(da) if the authorisation authorises the use of a tracking device for the purposes of an integrity operation—details identifying the integrity authority for the operation and each alleged relevant offence; and

(db) if the authorisation is given on the basis of a Part 5.3 supervisory order that is in force in relation to a person—the following details:

(i) the name of the person;

(ii) the date the order was made;

Authorised Version C2025C00651 registered 28/11/2025

(iii) if (disregarding section 6C) the order is not already in force and the order is not an interim control order—when the order comes into force;

(iv) whether the order is an interim control order, a confirmed control order, an interim supervision order or an extended supervision order; and

(dc) if the authorisation is given on the basis of a community safety supervision order that is in force in relation to a person—the following details:

(i) the name of the person;

(ii) the date the order was made;

(iii) if (disregarding section 6E) the order is not already in force—when the order comes into force; and

(e) if the authorisation authorises the use of a tracking device in or on an object or class of object—the object or class of object in or on which the use of the tracking device is authorised; and

(f) if the authorisation authorises the use of a tracking device on a vehicle or class of vehicle—the vehicle or class of vehicle on which the use of the tracking device is authorised; and

(g) if the authorisation authorises the use of a tracking device in respect of the conversations, activities or geographical location of a person—the name of the person (if known); and

(h) if the authorisation authorises the retrieval of a tracking device—the premises or object from which the tracking device is to be retrieved; and

(i) the name of the law enforcement officer primarily responsible for executing the authorisation; and

(j) any conditions subject to which a tracking device may be used, under the authorisation.

(2) A written record made under subsection (1) is not a legislative instrument.

Authorised Version C2025C00651 registered 28/11/2025

Part 5—Extraterritorial operation of warrants

41 Definitions

(1) In this Part:

appropriate consenting official, in relation to a foreign country:

(a) when used in section 42 or 43—means an official of that country having authority in that country to give consent to the use of surveillance devices in that country or on a vessel or aircraft registered under the laws of that country; or

(b) when used in section 43A, 43B, 43C, 43D or 43E—means an official of that country having authority in that country to give consent to access to data held in computers in that country or on a vessel or aircraft registered under the laws of that country.

Australian fishing zone means the Australian fishing zone within the meaning of the *Fisheries Management Act 1991*.

42 Extraterritorial operation of surveillance device warrants

(1) If, before the issue of a surveillance device warrant in relation to the investigation of a relevant offence on an application made by or on behalf of a federal law enforcement officer, it becomes apparent to the applicant that there will be a need for surveillance:

(a) in a foreign country; or

(b) on a vessel or aircraft that is registered under the law of a foreign country and is in or above waters beyond the outer limits of the territorial sea of Australia;

to assist in that investigation, the eligible Judge or nominated ART member considering the application for the warrant must not permit the warrant to authorise that surveillance unless the Judge or member is satisfied that the surveillance has been agreed to by an appropriate consenting official of the foreign country.

Authorised Version C2025C00651 registered 28/11/2025

(2) If:

(a) application is made under section 33 by an appropriate authorising officer who is a federal law enforcement officer for approval of the giving of an emergency authorisation relating to the investigation of a relevant offence; and

(aa) the emergency authorisation was given in response to an application under subsection 28(1); and

(b) before the completion of consideration of that section 33 application, it becomes apparent to the applicant that there will be a need for surveillance:

(i) in a foreign country; or

(ii) on a vessel or aircraft that is registered under the law of a foreign country and is in or above waters beyond the outer limits of the territorial sea of Australia;

to assist in the investigation to which the emergency authorisation related;

the eligible Judge or nominated ART member to whom the section 33 application was made must not permit any warrant issued on consideration of that section 33 application to authorise that surveillance unless the Judge or member is satisfied that the surveillance has been agreed to by an appropriate consenting official of the foreign country.

(3) If:

(a) a surveillance device warrant has been issued in relation to the investigation of a relevant offence on an application by or on behalf of a federal law enforcement officer; and

(b) after the issue of the warrant it becomes apparent to the law enforcement officer primarily responsible for executing the warrant that there will be a need for surveillance:

(i) in a foreign country; or

(ii) on a vessel or aircraft that is registered under the law of a foreign country and is in or above waters beyond the outer limits of the territorial sea of Australia;

to assist in that investigation;

Authorised Version C2025C00651 registered 28/11/2025

the warrant is taken to permit that surveillance if, and only if, the surveillance has been agreed to by an appropriate consenting official of the foreign country.

(4) Despite subsections (1), (2) and (3), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the contiguous zone of Australia; and

(b) the relevant offence in respect of which it becomes apparent that surveillance on the vessel will be required is an offence relating to the customs, fiscal, immigration or sanitary laws of Australia;

there is no requirement for the agreement of an appropriate consenting official of the foreign country concerned in relation to that surveillance while the vessel is in such waters.

(5) Despite subsections (1), (2) and (3), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the Australian fishing zone; and

(b) the relevant offence in respect of which it becomes apparent that surveillance on the vessel will be required is an offence against section 100, 100A, 100B, 101, 101A or 101AA of the *Fisheries Management Act 1991* or section 46A, 46B, 46C, 46D, 49A or 51A of the *Torres Strait Fisheries Act 1984*;

there is no requirement for the agreement of an appropriate consenting official of the foreign country concerned in relation to that surveillance while the vessel is in those waters.

(6) As soon as practicable after the commencement of surveillance under the authority of a surveillance device warrant:

(a) in a foreign country; or

(b) in circumstances where consent to that surveillance is required—on a vessel or aircraft that is registered under the law of a foreign country;

Authorised Version C2025C00651 registered 28/11/2025

the chief officer of the law enforcement agency to which the law enforcement officer who applied for the warrant belongs or is seconded must give the Minister evidence in writing that the surveillance has been agreed to by an appropriate consenting official of the foreign country.

(7) An instrument providing evidence of the kind referred to in subsection (6) is not a legislative instrument.

(8) If a vessel or aircraft that is registered under the laws of a foreign country is in or above the territorial sea of another foreign country, subsections (1), (2) and (3) have effect as if the reference to an appropriate consenting official of the foreign country were a reference to an appropriate consenting official of each foreign country concerned.

(9) For the avoidance of doubt, there is no requirement for the agreement of an appropriate consenting official of the foreign country to the surveillance under the authority of a surveillance device warrant of a vessel or aircraft of a foreign country that is in Australia or in or above waters within the outer limits of the territorial sea of Australia.

43 Evidence obtained from extraterritorial surveillance not to be tendered in evidence unless court satisfied properly obtained

Evidence obtained from surveillance undertaken in a foreign country in accordance with subsection 42(1), (2) or (3) in relation to a relevant offence cannot be tendered in evidence to a court in any proceedings relating to the relevant offence unless the court is satisfied that the surveillance was agreed to by an appropriate consenting official of the foreign country.

43A Extraterritorial operation of computer access warrants

(1) If, before the issue of a computer access warrant in relation to the investigation of a relevant offence in response to an application made by or on behalf of a federal law enforcement officer, it

Authorised Version C2025C00651 registered 28/11/2025

becomes apparent to the applicant that there will be a need for access to data held in a computer:

(a) in a foreign country; or

(b) on a vessel or aircraft that is registered under the law of a foreign country and is in or above waters beyond the outer limits of the territorial sea of Australia;

to assist in that investigation, the eligible Judge or nominated ART member considering the application for the warrant must not permit the warrant to authorise that access unless the eligible Judge or nominated ART member is satisfied that the access has been agreed to by an appropriate consenting official of the foreign country.

(2) If:

(a) application is made under section 33 by an appropriate authorising officer who is a federal law enforcement officer for approval of the giving of an emergency authorisation relating to the investigation of a relevant offence; and

(b) the emergency authorisation was given in response to an application under subsection 28(1A); and

(c) before the completion of consideration of that section 33 application, it becomes apparent to the applicant that there will be a need for access to data held in a computer:

(i) in a foreign country; or

(ii) on a vessel or aircraft that is registered under the law of a foreign country and is in or above waters beyond the outer limits of the territorial sea of Australia;

to assist in the investigation to which the emergency authorisation related;

the eligible Judge or nominated ART member to whom the section 33 application was made must not permit any computer access warrant issued on consideration of that section 33 application to authorise that access unless the eligible Judge or nominated ART member is satisfied that the access has been agreed to by an appropriate consenting official of the foreign country.

Authorised Version C2025C00651 registered 28/11/2025

(3) If:

(a) a computer access warrant has been issued in relation to the investigation of a relevant offence in response to an application by or on behalf of a federal law enforcement officer; and

(b) after the issue of the warrant, it becomes apparent to the law enforcement officer primarily responsible for executing the warrant that there will be a need for access to data held in a computer that is:

(i) in a foreign country; or

(ii) on a vessel or aircraft that is registered under the law of a foreign country and is in or above waters beyond the outer limits of the territorial sea of Australia;

to assist in that investigation;

the warrant is taken to permit that access if, and only if, the access has been agreed to by an appropriate consenting official of the foreign country.

(4) Subsections (1), (2) and (3) do not apply to a computer access warrant authorising access to data if:

(a) the person, or each of the persons, responsible for executing the warrant will be physically present in Australia; and

(b) the location where the data is held is unknown or cannot reasonably be determined.

(5) Despite subsections (1), (2) and (3), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the contiguous zone of Australia; and

(b) the relevant offence in respect of which it becomes apparent that access to data held in a computer on the vessel will be required is an offence relating to the customs, fiscal, immigration or sanitary laws of Australia;

there is no requirement for the agreement of an appropriate consenting official of the foreign country concerned in relation to that access while the vessel is in such waters.

Authorised Version C2025C00651 registered 28/11/2025

(6) Despite subsections (1), (2) and (3), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the Australian fishing zone; and

(b) the relevant offence in respect of which it becomes apparent that access to data held in a computer on the vessel will be required is an offence against section 100, 100A, 100B, 101, 101A or 101AA of the *Fisheries Management Act 1991* or section 46A, 46B, 46C, 46D, 49A or 51A of the *Torres Strait Fisheries Act 1984*;

there is no requirement for the agreement of an appropriate consenting official of the foreign country concerned in relation to that access while the vessel is in those waters.

(7) As soon as practicable after the commencement of access to data held in a computer under the authority of a computer access warrant in circumstances where consent to that access is required:

(a) in a foreign country; or

(b) on a vessel or aircraft that is registered under the law of a foreign country;

the chief officer of the law enforcement agency to which the law enforcement officer who applied for the warrant belongs or is seconded must give the Minister evidence in writing that the access has been agreed to by an appropriate consenting official of the foreign country.

(8) An instrument providing evidence of the kind referred to in subsection (7) is not a legislative instrument.

(9) If a vessel or aircraft that is registered under the laws of a foreign country is in or above the territorial sea of another foreign country, subsections (1), (2) and (3) have effect as if the reference to an appropriate consenting official of the foreign country were a reference to an appropriate consenting official of each foreign country concerned.

Authorised Version C2025C00651 registered 28/11/2025

(10) For the avoidance of doubt, there is no requirement for the agreement of an appropriate consenting official of the foreign country to the access to data held in a computer under the authority of a computer access warrant on a vessel or aircraft of a foreign country that is in Australia or in or above waters within the outer limits of the territorial sea of Australia.

43B Evidence obtained from extraterritorial computer access not to be tendered in evidence unless court satisfied properly obtained

Evidence obtained from access to data held in a computer undertaken in a foreign country in accordance with subsection 43A(1), (2) or (3) in relation to a relevant offence cannot be tendered in evidence to a court in any proceedings relating to the relevant offence unless the court is satisfied that the access was agreed to by an appropriate consenting official of the foreign country.

43C Extraterritorial operation of data disruption warrants

(1) If, before the issue of a data disruption warrant, it becomes apparent to the applicant for the warrant that there will be a need for access to, and disruption of, data held in a computer:

(a) in a foreign country; or

(b) on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limits of the territorial sea of Australia;

the eligible Judge or nominated ART member considering the application for the warrant must not permit the warrant to authorise that access and disruption unless the eligible Judge or nominated ART member is satisfied that the access and disruption has been agreed to by an appropriate consenting official of the foreign country.

(2) If:

Authorised Version C2025C00651 registered 28/11/2025

(a) an application is made under section 33 by an appropriate authorising officer for approval of the giving of an emergency authorisation; and

(b) the emergency authorisation was given in response to an application under subsection 28(1C); and

(c) before the completion of consideration of that section 33 application, it becomes apparent to the applicant that there will be a need for access to, and disruption of, data held in a computer:

(i) in a foreign country; or

(ii) on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limits of the territorial sea of Australia;

the eligible Judge or nominated ART member to whom the section 33 application was made must not permit any data disruption warrant issued on consideration of that section 33 application to authorise that access and disruption unless the eligible Judge or nominated ART member is satisfied that the access and disruption has been agreed to by an appropriate consenting official of the foreign country.

(3) If:

(a) a data disruption warrant has been issued; and

(b) after the issue of the warrant, it becomes apparent to the law enforcement officer primarily responsible for executing the warrant that there will be a need for access to, and disruption of, data held in a computer that is:

(i) in a foreign country; or

(ii) on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limits of the territorial sea of Australia;

the warrant is taken to permit that access and disruption if, and only if, the access and or disruption has been agreed to by an appropriate consenting official of the foreign country.

(4) Subsections (1), (2) and (3) do not apply to a data disruption warrant authorising access to, and disruption of, data if:

Authorised Version C2025C00651 registered 28/11/2025

(a) the person, or each of the persons, responsible for executing the warrant will be physically present in Australia; and

(b) the location where the data is held is unknown or cannot reasonably be determined.

(5) Despite subsections (1), (2) and (3), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the contiguous zone of Australia; and

(b) the relevant offences in respect of which it becomes apparent that access to, and disruption of, data held in a computer on the vessel will be required are offences relating to the customs, fiscal, immigration or sanitary laws of Australia;

there is no requirement for the agreement of an appropriate consenting official of the foreign country concerned in relation to that access or disruption while the vessel is in such waters.

(6) Despite subsections (1), (2) and (3), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the Australian fishing zone; and

(b) the relevant offences in respect of which it becomes apparent that access to, and disruption of, data held in a computer on the vessel will be required are offences against section 100, 100A, 100B, 101, 101A or 101AA of the *Fisheries Management Act 1991* or section 46A, 46B, 46C, 46D, 49A or 51A of the *Torres Strait Fisheries Act 1984*;

there is no requirement for the agreement of an appropriate consenting official of the foreign country concerned in relation to that access or disruption while the vessel is in those waters.

(7) As soon as practicable after the commencement of access to, and disruption of, data held in a computer under the authority of a data disruption warrant in circumstances where consent to that access or disruption is required:

(a) in a foreign country; or

Authorised Version C2025C00651 registered 28/11/2025

(b) on a vessel or aircraft that is registered under the law of a foreign country;

the chief officer of the law enforcement agency to which the law enforcement officer who applied for the warrant belongs or is seconded must give the Minister evidence in writing that the access and disruption has been agreed to by an appropriate consenting official of the foreign country.

(8) An instrument providing evidence of the kind referred to in subsection (7) is not a legislative instrument.

(9) If a vessel or aircraft that is registered under the laws of a foreign country is in or above the territorial sea of another foreign country, subsections (1), (2) and (3) have effect as if the reference to an appropriate consenting official of the foreign country were a reference to an appropriate consenting official of each foreign country concerned.

(10) For the avoidance of doubt, there is no requirement for the agreement of an appropriate consenting official of the foreign country to the access to, and disruption of, data held in a computer under the authority of a data disruption warrant on a vessel or aircraft of a foreign country that is in Australia or in or above waters within the outer limits of the territorial sea of Australia.

43D Evidence obtained from extraterritorial computer access not to be tendered in evidence unless court is satisfied that the evidence was properly obtained

Evidence obtained from access to, or disruption of, data held in a computer undertaken in a foreign country in accordance with subsection 43C(1), (2) or (3) in relation to a relevant offence cannot be tendered in evidence to a court in any proceedings relating to the relevant offence unless the court is satisfied that the access or disruption was agreed to by an appropriate consenting official of the foreign country.

Authorised Version C2025C00651 registered 28/11/2025

43E Extraterritorial operation of network activity warrants

(1) If, before the issue of a network activity warrant, it becomes apparent to the applicant that there will be a need for access to data held in a computer:

(a) in a foreign country; or

(b) on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limits of the territorial sea of Australia;

the eligible Judge or nominated ART member considering the application for the warrant must not permit the warrant to authorise that access unless the eligible Judge or nominated ART member is satisfied that the access has been agreed to by an appropriate consenting official of the foreign country.

(2) If:

(a) a network activity warrant has been issued; and

(b) after the issue of the warrant, it becomes apparent to the law enforcement officer primarily responsible for executing the warrant that there will be a need for access to data held in a computer that is:

(i) in a foreign country; or

(ii) on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limits of the territorial sea of Australia;

the warrant is taken to permit that access if, and only if, the access has been agreed to by an appropriate consenting official of the foreign country.

(3) Subsections (1) and (2) do not apply to a network activity warrant authorising access to data if:

(a) the person, or each of the persons, responsible for executing the warrant will be physically present in Australia; and

(b) the location where the data is held is unknown or cannot reasonably be determined.

(4) Despite subsections (1) and (2), if:

Authorised Version C2025C00651 registered 28/11/2025

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the contiguous zone of Australia; and

(b) the relevant offence in respect of which it becomes apparent that access to data held in a computer on the vessel will be required is an offence relating to the customs, fiscal, immigration or sanitary laws of Australia;

there is no requirement for the agreement of an appropriate consenting official of the foreign country concerned in relation to that access while the vessel is in such waters.

(5) Despite subsections (1) and (2), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the Australian fishing zone; and

(b) the relevant offence in respect of which it becomes apparent that access to data held in a computer on the vessel will be required is an offence against section 100, 100A, 100B, 101, 101A or 101AA of the *Fisheries Management Act 1991* or section 46A, 46B, 46C, 46D, 49A or 51A of the *Torres Strait Fisheries Act 1984*;

there is no requirement for the agreement of an appropriate consenting official of the foreign country concerned in relation to that access while the vessel is in those waters.

(6) As soon as practicable after the commencement of access to data held in a computer under the authority of a network activity warrant in circumstances where consent to that access is required:

(a) in a foreign country; or

(b) on a vessel or aircraft that is registered under the law of a foreign country;

the chief officer of the law enforcement agency to which the law enforcement officer who applied for the warrant belongs or is seconded must give the Minister evidence in writing that the access

Authorised Version C2025C00651 registered 28/11/2025

has been agreed to by an appropriate consenting official of the foreign country.

(7) An instrument providing evidence of the kind referred to in subsection (6) is not a legislative instrument.

(8) If a vessel or aircraft that is registered under the laws of a foreign country is in or above the territorial sea of another foreign country, subsections (1) and (2) have effect as if the reference to an appropriate consenting official of the foreign country were a reference to an appropriate consenting official of each foreign country concerned.

(9) For the avoidance of doubt, there is no requirement for the agreement of an appropriate consenting official of the foreign country to the access to data held in a computer under the authority of a network activity warrant on a vessel or aircraft of a foreign country that is in Australia or in or above waters within the outer limits of the territorial sea of Australia.

Authorised Version C2025C00651 registered 28/11/2025

Part 6—Compliance and monitoring

Division 1—Restrictions on use, communication and publication of information

44 What is protected information?

(1) In this Act:

protected information means:

(a) any information obtained from the use of a surveillance device under a warrant (other than a network activity warrant), an emergency authorisation or a tracking device authorisation; or

(aa) any information (other than general computer access intercept information) obtained from access to data under:

(i) a computer access warrant; or

(ii) an emergency authorisation for access to data held in a computer; or

(ab) any information (other than data disruption intercept information) obtained from access to, or disruption of, data under:

(i) a data disruption warrant; or

(ii) an emergency authorisation for disruption of data held in a computer; or

(b) any information relating to:

(i) an application for, the issue of, the existence of, or the expiration of, a warrant (other than a network activity warrant), an emergency authorisation or a tracking device authorisation; or

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

(c) any information that is likely to enable the identification of a person, object or premises specified in a warrant (other than a

Authorised Version C2025C00651 registered 28/11/2025

network activity warrant), an emergency authorisation or a tracking device authorisation; or

(d) any other information obtained by a law enforcement officer:

(i) without the authority of a warrant (other than a network activity warrant) or a tracking device authorisation; or

(ii) without the authority of an emergency authorisation that was subsequently approved; or

(iii) in a case where the information was obtained (otherwise than purportedly under a network activity warrant) through the use of a surveillance device in a foreign country, or on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limit of Australia's territorial sea—without the agreement of the appropriate consenting official of that foreign country, and of any other foreign country, whose agreement is required under section 42; or

(iv) in a case where the information was obtained, purportedly under a computer access warrant or an emergency authorisation for access to data held in a computer, through access to data held in a computer in a foreign country, or on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limit of Australia's territorial sea—without the agreement of the appropriate consenting official of that foreign country, and of any other foreign country, whose agreement is required under section 43A; or

(v) in a case where the information was obtained, purportedly under a data disruption warrant or an emergency authorisation for disruption of data held in a computer, through access to, or disruption of, data held in a computer in a foreign country, or on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limit of Australia's territorial sea—without the agreement of the appropriate consenting official of that

Authorised Version C2025C00651 registered 28/11/2025

foreign country, and of any other foreign country, whose agreement is required under section 43C;

in contravention of the requirement for a warrant (other than a network activity warrant), tracking device authorisation or emergency authorisation.

Note 1: For protection of general computer access intercept information, see Part 2-6 of the *Telecommunications (Interception and Access) Act 1979*.

Note 2: For protection of data disruption intercept information, see Part 2-6 of the *Telecommunications (Interception and Access) Act 1979*.

(2) For the avoidance of doubt, information obtained under an emergency authorisation falls under paragraph (a) and not paragraph (d) of the definition of ***protected information*** unless:

(a) an eligible Judge or nominated ART member refuses to approve the giving of the emergency authorisation; or

(b) contrary to the requirement of section 33, no application for such an approval has been made.

44A What is protected network activity warrant information?

For the purposes of this Act, ***protected network activity warrant information*** means:

(a) any information (other than network activity warrant intercept information) obtained from access to data under a network activity warrant; or

(b) any information obtained from the use of a surveillance device under a network activity warrant; or

(c) information relating to an application for, the issue of, the existence of, or the expiration of, a network activity warrant; or

(d) any information that is likely to enable the identification of:

(i) a criminal network of individuals specified in a network activity warrant; or

(ii) an individual in a criminal network of individuals specified in a network activity warrant; or

(iii) a computer specified in a network activity warrant; or

Authorised Version C2025C00651 registered 28/11/2025

(iv) premises specified in a network activity warrant; or

(e) any other information obtained by a law enforcement officer:

(i) without the authority of a network activity warrant; or

(ii) in a case where the information was obtained, purportedly under a network activity warrant, through access to data held in a computer in a foreign country, or on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limit of Australia's territorial sea—without the agreement of the appropriate consenting official of that foreign country, and of any other foreign country, whose agreement is required under section 43E;

in contravention of the requirement for a network activity warrant.

Note: For protection of network activity warrant intercept information, see Part 2-6 of the *Telecommunications (Interception and Access) Act 1979*.

45 Prohibition on use, recording, communication or publication of protected information or its admission in evidence

(1) A person commits an offence if:

(a) the person uses, records, communicates or publishes any information; and

(b) the information is protected information; and

(c) the use, recording, communication or publication of the information is not permitted by this section or section 45A (which deals with information relating to integrity operations) or section 65B (which deals with information obtained before an interim control order is declared void).

Penalty: Imprisonment for 2 years.

(2) A person commits an offence if:

(a) the person uses, records, communicates or publishes any information; and

Authorised Version C2025C00651 registered 28/11/2025

(b) the information is protected information; and

(c) the use, recording, communication or publication of the information is not permitted by this section or section 45A (which deals with information relating to integrity operations) or section 65B (which deals with information obtained before an interim control order is declared void); and

(d) the use, recording, communication or publication of the information, endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence.

Penalty: Imprisonment for 10 years.

(3) Subject to subsections (4) and (5) and section 65B, protected information may not be admitted in evidence in any proceedings.

(4) Subsections (1), (2) and (3) do not apply to:

(aa) the use, recording, communication or publication of protected information in connection with the administration or execution of this Act; or

(a) the use, recording, communication or publication of any information that has been disclosed in proceedings in open court lawfully; or

(b) the use or communication of protected information by a person who 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*) of protected information that relates or appears to relate to any matter within the functions of that organisation; or

(d) the communication to the agency head (within the meaning of the *Intelligence Services Act 2001*) of an agency (within the meaning of that Act) of protected information that relates

Authorised Version C2025C00651 registered 28/11/2025

or appears to relate to any matter within the functions of that agency; or

(e) the use, recording or communication of:

(i) protected information referred to in paragraph (c)—by the Director-General (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), an ASIO employee (within the meaning of that Act) or an ASIO affiliate (within the meaning of that Act); or

(ii) protected information referred to in paragraph (d)—by the agency head (within the meaning of the *Intelligence Services Act 2001*), or a staff member (within the meaning of that Act), of an agency (within the meaning of that Act);

in the performance of his or her official functions; or

(f) the communication of information for the purpose of providing it to one of the following entities (or to an appropriate authority of that entity):

(i) a foreign country;

(ii) the International Criminal Court;

(iii) a War Crimes Tribunal;

if the information was obtained under, or relates to, a surveillance device warrant issued in relation to an international assistance authorisation requested by that entity; or

(g) the communication of information for the purpose of providing it to a foreign country, or an appropriate authority of a foreign country, if this has been authorised under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987*; or

(h) the communication of information for the purpose of providing it to the International Criminal Court, if this has been authorised under section 69A of the *International Criminal Court Act 2002*; or

(i) the communication of information for the purpose of providing it to a War Crimes Tribunal, if this has been

Authorised Version C2025C00651 registered 28/11/2025

authorised under section 25A of the *International War Crimes Tribunals Act 1995*.

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

(a) the investigation of a relevant offence (including a State or Territory relevant offence but not including a relevant offence referred to in paragraph (d) or (i)) or the making of a report on the outcome of such an investigation;

(b) the making of a decision whether or not to bring a prosecution for a relevant offence (including a State or Territory relevant offence but not including a relevant offence referred to in paragraph (d) or (i));

(c) a relevant proceeding (not including a relevant proceeding in respect of a relevant offence referred to in paragraph (d) or (i)) or a State or Territory relevant proceeding;

(d) an investigation of a complaint against, or into the conduct of, a public officer within the meaning of this Act and also any subsequent investigation or prosecution of a relevant offence arising directly from the investigation of the complaint, or into the conduct;

(e) the making of a decision in relation to the appointment, term of appointment, termination of the appointment, or retirement, of a person referred to in paragraph (d);

(f) the keeping of records and the making of reports by a law enforcement agency under Division 2;

(g) an inspection by the Ombudsman under section 55;

(h) the performance of any function of the public interest monitor under either the *Crime and Corruption Act 2001* of Queensland or the *Police Powers and Responsibilities Act 2000* of Queensland or under both of those Acts with respect to ensuring compliance with either of those Acts or with this Act;

(i) an investigation under the *Privacy Act 1988* or any other law of the Commonwealth concerning the privacy of personal information and also any subsequent investigation or

Authorised Version C2025C00651 registered 28/11/2025

prosecution of a relevant offence arising directly from that first-mentioned investigation;

(ia) the performance of a function or duty, or the exercise of a power, by a person, court or other body under, or in relation to a matter arising under:

(i) Division 104 (control orders), Division 105A (post-sentence orders) or Division 395 (community safety orders) of the *Criminal Code*; or

(ii) a post-sentence detention law or a post-sentence supervision law; or

(iii) section 36C of the *Australian Citizenship Act 2007*;

(j) in the case of information:

(i) obtained under a warrant issued on the basis of a Part 5.3 supervisory order that is or was in force; or

(ii) relating to an application for, the issue of, the existence of, or the expiration of, such a warrant; or

(iii) that is likely to enable the identification of a person, object or premises specified in such a warrant;

determining whether the order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;

(k) in the case of information:

(i) obtained under a tracking device authorisation given on the basis of a Part 5.3 supervisory order; or

(ii) relating to an application for, the giving of, the existence of, or the expiration of, a tracking device authorisation given on the basis of a Part 5.3 supervisory order; or

(iii) that is likely to enable the identification of a person, object or premises specified in a tracking device authorisation given on the basis of a Part 5.3 supervisory order;

determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with;

(ka) in the case of information:

Authorised Version C2025C00651 registered 28/11/2025

(i) obtained under a warrant issued on the basis of a community safety supervision order that is or was in force; or

(ii) relating to an application for, the issue of, the existence of, or the expiration of, such a warrant; or

(iii) that is likely to enable the identification of a person, object or premises specified in such a warrant;

determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with;

(kb) in the case of information:

(i) obtained under a tracking device authorisation given on the basis of a community safety supervision order; or

(ii) relating to an application for, the giving of, the existence of, or the expiration of, a tracking device authorisation given on the basis of a community safety supervision order; or

(iii) that is likely to enable the identification of a person, object or premises specified in a tracking device authorisation given on the basis of a community safety supervision order;

determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with;

(l) an IGIS official exercising powers, or performing functions or duties, as an IGIS official.

(5A) To avoid doubt, paragraphs (5)(ia), (j) and (ka) do not limit paragraph (5)(c).

Note: Under paragraph (5)(c), protected information obtained under a warrant or authorisation may be used for the purposes of any proceedings relating to a post-sentence order or a Part 9.10 order.

Authorised Version C2025C00651 registered 28/11/2025

(6) Paragraphs (4)(f) and (g) and (5)(a), (b), (c) and (ia) to (kb) do not authorise:

(a) the use, recording, communication or publication of information of the kind referred to in paragraph (d) of the definition of ***protected information*** in section 44; or

(b) the giving in evidence of protected information of the kind referred to in paragraph (d) of that definition;

regardless of whether that information is also information of the kind referred to in paragraph (b) or (c) of that definition.

(6A) Protected information may be communicated by an Ombudsman official to an IGIS official for the purposes of the IGIS official exercising powers, or performing functions or duties, as an IGIS official.

(7) If protected information obtained through the use of a surveillance device by a law enforcement officer of a particular law enforcement agency (the ***originating agency***):

(a) is communicated to another law enforcement agency (by communicating it to the chief officer or another officer of that agency); or

(b) is communicated to any agency that is not a law enforcement agency (other than the Australian Security Intelligence Organisation and the agencies within the meaning of the *Intelligence Services Act 2001*) (by communicating it to the officer in charge of that agency or to another officer of that agency);

for a particular purpose, the protected information that has been so communicated:

(c) may be communicated from one officer to another within that agency or organisation for that purpose only; and

(d) must not, except for the purpose of bringing a relevant proceeding, or a State or Territory relevant proceeding, be communicated to any person who is not a member of that agency or organisation.

(8) A reference in subsection (5) to a relevant offence is a reference to any relevant offence, whether or not the offence in respect of

Authorised Version C2025C00651 registered 28/11/2025

which the relevant warrant or emergency authorisation was issued or given.

(9) In this section:

State or Territory relevant offence means a relevant offence against the law of a State or self-governing Territory that is punishable by a maximum term of imprisonment of 3 years or more or for life.

State or Territory relevant proceeding means:

(a) the prosecution of a State or Territory relevant offence; or

(b) a proceeding for the confiscation, forfeiture or restraint of property, or for the imposition of a pecuniary penalty, in relation to a State or Territory relevant offence; or

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

(d) a disciplinary offence against a public officer; or

(e) 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 State or Territory relevant offence; or

(f) a proceeding by way of a bail application that relates to a proceeding by way of a prosecution for a State or Territory relevant offence; or

(g) a proceeding for a review of a decision to refuse such a bail application; or

(h) a proceeding for a review of a decision to grant such a bail application; or

(i) a proceeding under, or a proceeding relating to a matter arising under, a preventative detention order law (other than Division 105 of the *Criminal Code*), so far as the proceeding relates to a preventative detention order (within the meaning of that preventative detention order law); or

(j) a proceeding under, or a proceeding relating to a matter arising under, a post-sentence detention law or a post-sentence supervision law.

Authorised Version C2025C00651 registered 28/11/2025

45A Protected information related to integrity operations

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

(a) making a decision about whether to apply for an integrity authority;

(b) designing an integrity operation;

(c) applying for an integrity authority;

(d) granting an integrity authority;

(e) conducting an integrity operation;

(f) applying for any warrant, authorisation or order, under a law of the Commonwealth, for the purposes of an integrity operation;

(g) any disciplinary or legal action in relation to a staff member of a target agency, if arising out of, or otherwise related to, an integrity testing operation.

Note: If use etc. of protected information is permitted under this section, the offences in subsections 45(1) and (2) do not apply (see paragraphs 45(1)(c) and (2)(c)).

(2) Subsection (1) does not limit subsections 45(4) and (5) (which permit protected information to be used etc. for certain other purposes).

(3) If protected information is communicated under subsection (1), subsection 45(7) does not apply in relation to the further communication of the information.

Note: If protected information is communicated from one agency to another agency, subsection 45(7) restricts the circumstances in which the information may be further communicated.

(4) Paragraph (1)(g) (use etc. for disciplinary or legal action) does not authorise:

(a) the use, recording, communication or publication of information of the kind referred to in paragraph (d) of the definition of ***protected information*** in section 44; or

Authorised Version C2025C00651 registered 28/11/2025

(b) the giving in evidence of protected information of the kind referred to in paragraph (d) of that definition;

regardless of whether that information is also information of the kind referred to in paragraph (b) or (c) of that definition.

Note: Paragraph (d) of the definition of ***protected information*** in section 44 covers information obtained by a law enforcement officer in contravention of a requirement for a warrant, tracking device authorisation or emergency authorisation.

(5) In this section:

disciplinary or legal action, in relation to a staff member of a target agency, means any of the following:

(a) action in respect of alleged misconduct of the staff member;

(b) termination of the employment or appointment of the staff member;

(c) a disciplinary proceeding in relation to the staff member, or a report of such a proceeding;

(d) the investigation of an offence suspected to have been committed by the staff member;

(e) a legal proceeding in relation to the staff member, or a report of such a proceeding.

Disciplinary or legal action also includes the consideration of whether an action or proceeding covered by this definition should be taken or brought.

staff member, of a target agency, means a staff member of that agency within the meaning of section 12 of the *National Anti-Corruption Commission Act 2022*.

45B Prohibition on use, recording, communication or publication of protected network activity warrant information or its admission in evidence

(1) A person commits an offence if:

(a) the person uses, records, communicates or publishes any information; and

Authorised Version C2025C00651 registered 28/11/2025

(b) the information is protected network activity warrant information; and

(c) the use, recording, communication or publication of the information is not permitted by this section.

Penalty: Imprisonment for 2 years.

(2) A person commits an offence if:

(a) the person uses, records, communicates or publishes any information; and

(b) the information is protected network activity warrant information; and

(c) the use, recording, communication or publication of the information is not permitted by this section; and

(d) the use, recording, communication or publication of the information:

(i) endangers the health or safety of any person; or

(ii) prejudices the effective conduct of an investigation into a relevant offence.

Penalty: Imprisonment for 10 years.

(3) Subject to subsections (4), (5), (7) and (10), protected network activity warrant information may not be admitted in evidence in any proceedings.

(4) Subsections (1), (2) and (3) do not apply to:

(a) the use, recording, communication or publication of protected network activity warrant information in connection with the administration or execution of this Act; or

(b) the use, recording, communication or publication of any information that has been disclosed in proceedings in open court lawfully; or

(c) the use or communication of protected network activity warrant information by a person who 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

Authorised Version C2025C00651 registered 28/11/2025

(d) the communication to the Director-General (within the meaning of the *Australian Security Intelligence Organisation Act 1979*) of protected network activity warrant information that relates or appears to relate to any matter within the functions of that organisation; or

(e) the communication to the agency head (within the meaning of the *Intelligence Services Act 2001*) of an agency (within the meaning of that Act) of protected network activity warrant information that relates or appears to relate to any matter within the functions of that agency; or

(f) the use, recording or communication of:

(i) protected network activity warrant information referred to in paragraph (d)—by the Director-General (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), an ASIO employee (within the meaning of that Act) or an ASIO affiliate (within the meaning of that Act); or

(ii) protected network activity warrant information referred to in paragraph (e)—by the agency head (within the meaning of the *Intelligence Services Act 2001*), or a staff member (within the meaning of that Act), of an agency (within the meaning of that Act);

in the performance of the official functions of the Director-General, ASIO employee, ASIO affiliate, agency head or staff member, as the case may be.

(5) Protected network activity warrant information (other than information that was obtained from the use of a surveillance device under a network activity warrant) may be used, recorded, communicated or published, or may be admitted in evidence, if it is necessary to do so for any of the following purposes:

(a) the purposes of the Australian Federal Police collecting, correlating, analysing or disseminating criminal intelligence in the performance of the functions conferred by section 8 of the *Australian Federal Police Act 1979*;

(b) the purposes of the Australian Crime Commission collecting, correlating, analysing or disseminating criminal intelligence

Authorised Version C2025C00651 registered 28/11/2025

in the performance of the functions conferred by section 7A of the *Australian Crime Commission Act 2002*;

(c) the purposes of the Australian Federal Police or the Australian Crime Commission making reports in relation to criminal intelligence;

(d) the making of an application for a warrant;

(e) the making of an application for the variation of a warrant;

(f) the making of an application for the extension of a warrant;

(g) the keeping of records and the making of reports by the Australian Federal Police or the Australian Crime Commission under Division 2;

(h) the purposes of an IGIS official exercising powers, or performing functions or duties, as an IGIS official;

(i) the purposes of an investigation of an offence against subsection (1) or (2);

(j) a proceeding relating to an offence against subsection (1) or (2).

(6) The definition of ***warrant*** in subsection 6(1) does not apply to paragraphs (5)(d), (e) and (f) of this section.

Note: This means that warrant has its ordinary meaning.

(7) Protected network activity warrant information that was obtained from the use of a surveillance device under a network activity warrant may be used, recorded, communicated or published, or may be admitted in evidence, if it is necessary to do so for any of the following purposes:

(a) the purposes of doing a thing authorised by a network activity warrant;

(b) the purposes of an IGIS official exercising powers, or performing functions or duties, as an IGIS official;

(c) the purposes of an investigation of an offence against subsection (1) or (2);

(d) a proceeding relating to an offence against subsection (1) or (2).

Authorised Version C2025C00651 registered 28/11/2025

(8) Protected network activity warrant information may be communicated by an Ombudsman official to an IGIS official for the purposes of the IGIS official exercising powers, or performing functions or duties, as an IGIS official.

(9) Protected network activity warrant information may be communicated by an IGIS official to an Ombudsman official for the purposes of the Ombudsman official exercising powers, or performing functions or duties, as an Ombudsman official.

(9A) Protected network activity warrant information may be used, recorded or communicated for the purposes of the making of a decision whether or not to bring, or continue, a prosecution for a relevant offence.

(9B) Protected network activity warrant information may be used, recorded or communicated:

(a) for the purposes of complying with any applicable common law or statutory disclosure duty or obligation in a criminal proceeding for a relevant offence; or

(b) if, under paragraph (a), the information is communicated to the legal representative of a defendant in a proceeding—by the legal representative for the purposes of representing the defendant in the proceeding.

(10) Protected network activity warrant information may be admitted in evidence in:

(a) a criminal proceeding for an offence against subsection (1) or (2); or

(ab) a criminal proceeding for a relevant offence if the circumstances in subsection (10A) apply; or

(b) a proceeding that is not a criminal proceeding.

(10A) For the purposes of paragraph (10)(ab), the circumstances are:

(a) both of the following apply:

(i) the protected network activity warrant information is adduced or given in evidence in the proceeding by a defendant in the proceeding;

Authorised Version C2025C00651 registered 28/11/2025

(ii) the admission into evidence of the information is necessary for the fair trial of the defendant; or

(b) the protected network activity warrant information is adduced or given in evidence in the proceeding by the prosecution in the proceeding in response to other protected network activity warrant information admitted into evidence in that proceeding in the circumstances mentioned in paragraph (a).

(11) If:

(a) protected network activity warrant information was obtained from access to data, or the use of a surveillance device, under a network activity warrant; and

(b) the warrant was granted in response to an application made by the chief officer of a particular law enforcement agency; and

(c) the information:

(i) is communicated to another law enforcement agency (by communicating it to the chief officer or another officer of that agency) for a particular purpose; or

(ii) is communicated to any agency that is not a law enforcement agency (other than the Office of the Inspector-General of Intelligence and Security, the Australian Security Intelligence Organisation and the agencies within the meaning of the *Intelligence Services Act 2001*) (by communicating it to the officer in charge of that agency or to another officer of that agency) for a particular purpose;

the information that has been so communicated:

(d) may be communicated from one officer to another within that agency for that purpose only; and

(e) must not be communicated to any person who is not an officer of that agency.

Authorised Version C2025C00651 registered 28/11/2025

46 Dealing with records obtained by using a surveillance device or accessing data held in a computer

(1) The chief officer of a law enforcement agency:

(a) must ensure that every record or report comprising protected information, general computer access intercept information or data disruption intercept information is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report; and

(b) must cause to be destroyed any record or report referred to in paragraph (a):

(i) as soon as practicable after the making of the record or report if the chief officer is satisfied that no civil or criminal proceeding to which the material contained in the record or report relates has been, or is likely to be, commenced and that the material contained in the record or report is not likely to be required in connection with an activity referred to in subsection 45(4) or a purpose referred to in subsection 45(5) or 45A(1); and

(ii) within the period of 5 years after the making of the record or report, and within each period of 5 years thereafter, unless, before the end of that period, the chief officer is satisfied in relation to the material contained in the record or report of a matter referred to in subparagraph (i) and certifies to that effect.

(2) If an agency is not a law enforcement agency but, as described in subsection 45(4) or (5) or 45A(1), receives records or reports obtained by:

(aa) using a surveillance device; or

(ab) accessing data held in a computer; or

(ac) disrupting data held in a computer;

the officer in charge of the agency:

(a) must ensure that every record or report that is so received is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report; and

Authorised Version C2025C00651 registered 28/11/2025

(b) must cause to be destroyed any record or report referred to in paragraph (a):

(i) as soon as practicable after the receipt of the record or report by the agency if the officer in charge is satisfied that no civil or criminal proceeding to which the material contained in the record or report relates has been, or is likely to be, commenced and that the material contained in the record or report is not likely to be required in connection with an activity referred to in subsection 45(4) or a purpose referred to in subsection 45(5) or 45A(1); and

(ii) within the period of 5 years after the making of the record or report, and within each period of 5 years thereafter, unless, before the end of that period, the officer in charge is satisfied in relation to the material contained in the record or report of a matter referred to in subparagraph (i) and certifies to that effect.

(3) Subsections (1) and (2) do not apply to a record or report that is received into evidence in legal proceedings or disciplinary proceedings.

46AA Dealing with records obtained by accessing data under a network activity warrant

(1) The chief officer of the Australian Federal Police or the Australian Crime Commission:

(a) must ensure that every record or report comprising:

(i) protected network activity warrant information; or

(ii) network activity warrant intercept information;

is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report; and

(b) must cause to be destroyed any record or report referred to in paragraph (a):

(i) as soon as practicable after the making of the record or report if the chief officer is satisfied that no civil or criminal proceeding to which the material contained in

Authorised Version C2025C00651 registered 28/11/2025

the record or report relates has been, or is likely to be, commenced and that the material contained in the record or report is not likely to be required in connection with an activity referred to in subsection 45B(4) or a purpose referred to in subsection 45B(5) or (7); and

(ii) within the period of 5 years after the making of the record or report, and within each period of 5 years thereafter, unless, before the end of that period, the chief officer is satisfied in relation to the material contained in the record or report of a matter referred to in subparagraph (i) and certifies to that effect.

(2) If an agency is not a law enforcement agency but, as described in subsection 45B(5) or (7), receives records or reports obtained by accessing data, or using a surveillance device, under a network activity warrant, the officer in charge of the agency:

(a) must ensure that every record or report that is so received is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report; and

(b) must cause to be destroyed any record or report referred to in paragraph (a):

(i) as soon as practicable after the receipt of the record or report by the agency if the officer in charge is satisfied that no civil or criminal proceeding to which the material contained in the record or report relates has been, or is likely to be, commenced and that the material contained in the record or report is not likely to be required in connection with an activity referred to in subsection 45B(4) or a purpose referred to in subsection 45B(5) or (7); and

(ii) within the period of 5 years after the making of the record or report, and within each period of 5 years thereafter, unless, before the end of that period, the officer in charge is satisfied in relation to the material contained in the record or report of a matter referred to in subparagraph (i) and certifies to that effect.

Authorised Version C2025C00651 registered 28/11/2025

(3) Subsection (2) does not apply to the Office of the Inspector-General of Intelligence and Security.

46A Destruction of records—information obtained before a Part 5.3 supervisory order came into force

(1) If:

(a) a record or report is in the possession of a law enforcement agency; and

(b) the record or report comprises information obtained from the use of a surveillance device under:

(i) a surveillance device warrant; or

(ii) a tracking device authorisation;

issued or given on the basis of a Part 5.3 supervisory order made in relation to a person; and

(c) in the case of a surveillance device warrant issued on the basis that a Part 5.3 supervisory order was in force—the warrant was issued for the purpose, or for purposes that include the purpose, of obtaining information that would be likely to substantially assist in connection with determining whether the order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and

(d) in the case of a tracking device authorisation—the authorisation was given to obtain information relating to the person for the purpose, or for purposes that include the purpose, of determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and

(e) the use of the surveillance device occurred when the Part 5.3 supervisory order had been made, but had not come into force; and

(f) the chief officer of the agency is satisfied that none of the information obtained from the use of the surveillance device is likely to assist in connection with achieving a Part 5.3 object;

Authorised Version C2025C00651 registered 28/11/2025

the chief officer of the agency must cause the record or report to be destroyed as soon as practicable.

(1A) If:

(a) a record or report is in the possession of a law enforcement agency; and

(b) the record or report comprises information obtained from access to data under a computer access warrant issued on the basis of a Part 5.3 supervisory order made in relation to a person; and

(c) the warrant was issued for the purpose, or for purposes that include the purpose, of obtaining information that would be likely to substantially assist in connection with determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and

(d) access to the data occurred when the Part 5.3 supervisory order had been made, but had not come into force; and

(e) the chief officer of the agency is satisfied that none of the information obtained from accessing the data is likely to assist in connection with achieving a Part 5.3 object;

the chief officer of the agency must cause the record or report to be destroyed as soon as practicable.

(2) Section 6C does not apply to subsection (1) or (1A) of this section.

46B Destruction of records—information obtained before a community safety supervision order came into force

(1) If:

(a) a record or report is in the possession of a law enforcement agency; and

(b) the record or report comprises information obtained from the use of a surveillance device under:

(i) a surveillance device warrant; or

(ii) a tracking device authorisation;

Authorised Version C2025C00651 registered 28/11/2025

issued or given on the basis of a community safety supervision order made in relation to a person; and

(c) in the case of a surveillance device warrant issued on the basis that a community safety supervision order was in force—the warrant was issued for the purpose, or for purposes that include the purpose, of obtaining information that would be likely to substantially assist in connection with determining whether the order, or any succeeding community safety supervision order, has been, or is being, complied with; and

(d) in the case of a tracking device authorisation—the authorisation was given to obtain information relating to the person for the purpose, or for purposes that include the purpose, of determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with; and

(e) the use of the surveillance device occurred when the community safety supervision order had been made, but had not come into force; and

(f) the chief officer of the agency is satisfied that none of the information obtained from the use of the surveillance device is likely to assist in connection with achieving a Part 9.10 object;

the chief officer of the agency must cause the record or report to be destroyed as soon as practicable.

(2) If:

(a) a record or report is in the possession of a law enforcement agency; and

(b) the record or report comprises information obtained from access to data under a computer access warrant issued on the basis of a community safety supervision order made in relation to a person; and

(c) the warrant was issued for the purpose, or for purposes that include the purpose, of obtaining information that would be likely to substantially assist in connection with determining whether the community safety supervision order, or any

Authorised Version C2025C00651 registered 28/11/2025

succeeding community safety supervision order, has been, or is being, complied with; and

(d) access to the data occurred when the community safety supervision order had been made, but had not come into force; and

(e) the chief officer of the agency is satisfied that none of the information obtained from accessing the data is likely to assist in connection with achieving a Part 9.10 object;

the chief officer of the agency must cause the record or report to be destroyed as soon as practicable.

(3) Section 6E does not apply to subsection (1) or (2) of this section.

47 Protection of surveillance device technologies and methods

(1) In a 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, he or she 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

Authorised Version C2025C00651 registered 28/11/2025

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 he or she 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 proceeding before a court, tribunal or Royal Commission.

47A Protection of computer access technologies and methods

(1) In a 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 computer access technologies or methods.

(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

Authorised Version C2025C00651 registered 28/11/2025

could reasonably be expected to reveal details of computer access technologies or methods, 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:

computer access technologies or methods means:

(a) technologies or methods relating to the use of:

(i) a computer; or

(ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or

(iii) any other electronic equipment; or

(iv) a data storage device;

for the purpose of obtaining access to data held in the computer; or

(b) technologies or methods relating to adding, copying, deleting or altering other data in a computer, if doing so is necessary to achieve the purpose mentioned in paragraph (a);

where the technologies or methods have been, or are being, deployed in giving effect to:

(c) a computer access warrant; or

(ca) a network activity warrant; or

(d) an emergency authorisation given in response to an application under subsection 28(1A), 29(1A) or 30(1A).

proceeding includes a proceeding before a court, tribunal or Royal Commission.

47B Protection of data disruption technologies and methods

(1) In a proceeding, a person may object to the disclosure of information on the ground that the information, if disclosed, could

Authorised Version C2025C00651 registered 28/11/2025

reasonably be expected to reveal details of data disruption technologies or methods.

(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 data disruption technologies or methods, 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:

data disruption technologies or methods means technologies or methods relating to the use of:

(a) a computer; or

(b) a telecommunications facility operated or provided by the Commonwealth or a carrier; or

(c) any other electronic equipment; or

Authorised Version C2025C00651 registered 28/11/2025

(d) a data storage device;

for either or both of the following purposes:

(e) disrupting data held in the computer;

(f) obtaining access to data held in the computer;

where the technologies or methods have been, or are being, deployed in giving effect to:

(g) a data disruption warrant; or

(h) an emergency authorisation for disruption of data held in a computer.

proceeding includes a proceeding before a court, tribunal or Royal Commission.

48 Protected information in the custody of a court, tribunal or Royal Commission

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

Authorised Version C2025C00651 registered 28/11/2025

Division 2—Reporting and record-keeping

49 Report on each warrant or authorisation

(1) The chief officer of each law enforcement agency to which there belongs or is seconded a law enforcement officer to whom:

(a) a warrant is issued; or

(b) an emergency authorisation is given; or

(c) a tracking device authorisation is given;

must, as soon as practicable after the warrant or authority ceases to be in force:

(d) make a report to the Minister in accordance with this section; and

(e) give to the Minister a copy of each such warrant or authorisation, and of any instrument revoking, extending or varying such a warrant or authorisation.

(2) In the case of a surveillance device warrant, or an emergency authorisation for the use of a surveillance device, or a tracking device authorisation, the report must:

(a) state whether the warrant or authorisation was executed; and

(b) if so:

(i) state the name of the person primarily responsible for the execution of the warrant or authorisation; and

(ii) state the name of each person involved in the installation, maintenance or retrieval of the surveillance device; and

(iii) state the kind of surveillance device used; and

(iv) state the period during which the device was used; and

(v) state 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; and

(vi) state the name, if known, of any person whose location was determined by the use of a tracking device; and

Authorised Version C2025C00651 registered 28/11/2025

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

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

(ix) if the warrant is issued or the authorisation given in respect of the investigation of a relevant offence—give 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; and

(x) if the warrant is issued or the authorisation given in respect of the location and safe recovery of a child to whom a recovery order relates—give details of use of the device in assisting with the location and safe recovery of the child; and

(xa) if the warrant is issued or the authorisation given for the purposes of an integrity operation—give details of the benefit to the operation 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; and

(xb) if the warrant is a Part 5.3 warrant—give the details specified in subsection (2A); and

(xc) if the warrant is a Part 9.10 warrant—give the details specified in subsection (2AA); and

(xi) give details of the communication of evidence or information obtained by the use of the device to persons other than officers of the agency; and

(xii) give details of the compliance with the conditions (if any) to which the warrant or authorisation was subject; and

(c) if the warrant or authorisation was extended or varied, state:

(i) the number of extensions or variations; and

(ii) the reasons for them.

(2A) For the purposes of subparagraph (2)(b)(xb), the details are:

Authorised Version C2025C00651 registered 28/11/2025

(aa) if the warrant was issued to determine whether to apply for a post-sentence order—the benefit of the use of the device in determining whether to make the application; and

(a) if the warrant was issued on the basis of a Part 5.3 supervisory order that is or was in force in relation to a person—the benefit of the use of the device in:

(i) achieving a Part 5.3 object; or

(ii) determining whether the Part 5.3 supervisory order has been, or is being, complied with; and

(b) the general use to be made of any evidence or information obtained by the use of the device.

(2AA) For the purposes of subparagraph (2)(b)(xc), the details are:

(a) if the warrant was issued to determine whether to apply for a Part 9.10 order—the benefit of the use of the device in determining whether to make the application; and

(b) if the warrant was issued on the basis of a community safety supervision order that is or was in force in relation to a person—the benefit of the use of the device in:

(i) achieving a Part 9.10 object; or

(ii) determining whether the community safety supervision order has been, or is being, complied with; and

(c) the general use to be made of any evidence or information obtained by the use of the device.

(2B) In the case of a computer access warrant, or an emergency authorisation, for access to data held in a computer, the report must:

(a) state whether the warrant or authorisation was executed; and

(b) if so:

(i) state the name of the person primarily responsible for the execution of the warrant or authorisation; and

(ii) state the name of each person involved in accessing data under the warrant or authorisation; and

(iii) state the period during which the data was accessed; and

Authorised Version C2025C00651 registered 28/11/2025

(iv) state the name, if known, of any person whose data was accessed; and

(v) give details of any premises at which the computer was located; and

(vi) if the warrant is issued, or the authorisation is given, in respect of the investigation of a relevant offence—give details of the benefit to the investigation of the accessed data and of the general use made, or to be made, of any evidence or information obtained by the access to data; and

(vii) if the warrant is issued, or the authorisation is given, in respect of the location and safe recovery of a child to whom a recovery order relates—give details of the use of the accessed data in assisting with the location and safe recovery of the child; and

(viii) if the warrant is issued, or the authorisation is given, for the purposes of an integrity operation—give details of the benefit to the operation of the accessed data and of the general use made, or to be made, of any evidence or information obtained by the access to data; and

(ix) if the warrant is a Part 5.3 warrant—give the details specified in subsection (2C); and

(ixa) if the warrant is a Part 9.10 warrant—give the details specified in subsection (2CA); and

(x) give details of the communication of evidence or information obtained by access to data held in the computer to persons other than officers of the agency; and

(xi) give details of the compliance with the conditions (if any) to which the warrant or authorisation was subject; and

(c) if the warrant or authorisation was extended or varied, state:

(i) the number of extensions or variations; and

(ii) the reasons for them.

(2C) For the purposes of subparagraph (2B)(b)(ix), the details are:

Authorised Version C2025C00651 registered 28/11/2025

(aa) if the warrant was issued to determine whether to apply for a post-sentence order—the benefit of obtaining access to data held in the computer in determining whether to make the application; and

(a) if the warrant was issued on the basis of a Part 5.3 supervisory order that is or was in force in relation to a person—the benefit of obtaining access to data held in the computer in:

(i) achieving a Part 5.3 object; or

(ii) determining whether the Part 5.3 supervisory order has been, or is being, complied with; and

(b) the general use to be made of any evidence or information obtained by access to data held in the computer.

(2CA) For the purposes of subparagraph (2B)(b)(ixa), the details are:

(a) if the warrant was issued to determine whether to apply for a Part 9.10 order—the benefit of obtaining access to data held in the computer in determining whether to make the application; and

(b) if the warrant was issued on the basis of a community safety supervision order that is or was in force in relation to a person—the benefit of obtaining access to data held in the computer in:

(i) achieving a Part 9.10 object; or

(ii) determining whether the community safety supervision order has been, or is being, complied with; and

(c) the general use to be made of any evidence or information obtained by access to data held in the computer.

(2D) In the case of:

(a) a data disruption warrant for disruption of data held in a computer; or

(b) an emergency authorisation for disruption of data held in a computer;

the report must:

(c) state whether the warrant or authorisation was executed; and

Authorised Version C2025C00651 registered 28/11/2025

(d) if so:

(i) state the name of the person primarily responsible for the execution of the warrant or authorisation; and

(ii) state the name of each person involved in accessing or disrupting data under the warrant or authorisation; and

(iii) state the period during which the data was accessed or disrupted; and

(iv) state the name, if known, of any person whose data was accessed or disrupted; and

(v) give details of any premises at which the computer was located; and

(vi) give details of the benefit of the use of the warrant or authorisation in frustrating criminal activity; and

(vii) give details of the access to, and disruption of, data under the warrant or authorisation; and

(viii) give details of the compliance with the conditions (if any) to which the warrant or authorisation was subject; and

(e) if the warrant or authorisation was extended or varied, state:

(i) the number of extensions or variations; and

(ii) the reasons for them.

(2E) In the case of a network activity warrant for access to data held in a computer, the report must:

(a) state whether the warrant was executed; and

(b) if so:

(i) state the name of the person primarily responsible for the execution of the warrant; and

(ii) state the name of each person involved in accessing data under the warrant; and

(iii) state the period during which the data was accessed; and

(iv) state the name, if known, of any person whose data was accessed; and

(v) give details of any premises, if known, at which the computer was located; and

Authorised Version C2025C00651 registered 28/11/2025

(vi) give details of any use of a surveillance device under the warrant; and

(vii) give details of the extent to which the execution of the warrant has contributed to the prevention, detection or frustration of one or more kinds of relevant offences; and

(viii) give details of the extent to which the execution of the warrant has assisted the agency in carrying out its functions; and

(ix) give details of the communication of information obtained by accessing data under the warrant to persons other than officers of the agency; and

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

(xi) give details of the information that was obtained from access to data under the warrant; and

(xii) give details of how the information that was obtained under the warrant was used; and

(xiii) give details of whether the information that was obtained under the warrant was destroyed or retained under section 46AA; and

(xiv) give details of any premises accessed, telecommunications intercepted or computers removed from premises under the warrant; and

(xv) give details of any activities undertaken under subsection 27KP(8) in relation to the warrant; and

(xvi) give details of any assistance orders made under subsection 64A(6A) in relation to the warrant; and

(c) if the warrant was extended or varied, state:

(i) the number of extensions or variations; and

(ii) the reasons for them.

(3) In the case of a retrieval warrant, the report must:

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

Authorised Version C2025C00651 registered 28/11/2025

(b) state whether the surveillance device was retrieved under the warrant; and
(c) if the device was not retrieved, state the reason why; and
(d) give details of the compliance with the conditions (if any) to which the warrant was subject.

49A Notification to Ombudsman in relation to Part 5.3 warrants or Part 9.10 warrants

(1) Within 6 months after a Part 5.3 warrant or a Part 9.10 warrant is issued in response to an application by a law enforcement officer of a law enforcement agency, the chief officer of the agency must:
(a) notify the Ombudsman that the warrant has been issued; and
(b) give the Ombudsman a copy of the warrant.

(2) As soon as practicable after the law enforcement agency, or a law enforcement officer of the law enforcement agency, contravenes any of the following conditions or provisions, the chief officer of the agency must notify the Ombudsman of the contravention:
(a) a condition specified in the warrant;
(b) any of the following provisions, to the extent that they relate to the warrant:
(i) subsection 20(2);
(ii) subsection 27G(2);
(iii) section 45;
(iv) subsection 46(1);
(c) section 46A;
(ca) section 46B;
(d) subsection 50A(4).

(3) A failure to comply with subsection (1) or (2) does not affect the validity of the warrant.

(4) This section applies in relation to a tracking device authorisation given on the basis of a Part 5.3 supervisory order, or a community safety supervision order, that is or was in force in the same way as

Authorised Version C2025C00651 registered 28/11/2025

this section applies in relation to a surveillance device warrant or computer access warrant.

49B Notification to Ombudsman in relation to concealment of access under a computer access warrant

If:

(a) a computer access warrant was issued in response to an application made by a law enforcement officer of a law enforcement agency; and

(b) a thing mentioned in subsection 27E(7) was done under the warrant after the 28-day period mentioned in paragraph 27E(7)(j);

the chief officer of the law enforcement agency must:

(c) notify the Ombudsman:

(i) that the warrant was issued; and

(ii) of the fact that the thing was done under the warrant after the 28-day period mentioned in paragraph 27E(7)(j); and

(d) do so within 7 days after the thing was done.

49C Notification to Ombudsman of things done under a data disruption warrant

(1) If:

(a) a data disruption warrant was issued in response to an application made by a law enforcement officer of a law enforcement agency; and

(b) a thing mentioned in subsection 27KE(2) was done under the warrant;

the chief officer of the law enforcement agency must:

(c) notify the Ombudsman:

(i) that the warrant was issued; and

(ii) of the fact that the thing was done under the warrant; and

(d) do so within 7 days after the thing was done.

Authorised Version C2025C00651 registered 28/11/2025

(2) If:

(a) a data disruption warrant was issued in response to an application made by a law enforcement officer of a law enforcement agency; and

(b) the person executing the warrant becomes aware that a thing mentioned in subsection 27KE(2) that was done under the warrant has caused material loss or damage to one or more persons lawfully using a computer;

the chief officer of the law enforcement agency must:

(c) notify the Ombudsman:

(i) that the thing has caused material loss or damage to one or more persons lawfully using a computer; and

(ii) of the particulars of that loss or damage; and

(d) do so within 7 days after the person executing the warrant became so aware.

49D Notification to Inspector-General of Intelligence and Security of things done under a network activity warrant

If:

(a) a network activity warrant was issued in response to an application made by the chief officer of the Australian Federal Police or the Australian Crime Commission; and

(b) a thing mentioned in subsection 27KP(8) was done under the warrant after the 28-day period mentioned in paragraph 27KP(8)(k);

the chief officer must:

(c) notify the Inspector-General of Intelligence and Security of the fact that the thing was done under the warrant after the 28-day period mentioned in paragraph 27KP(8)(k); and

(d) do so within 7 days after the thing was done.

Authorised Version C2025C00651 registered 28/11/2025

50 Annual reports

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

(a) the number of applications for warrants made by or on behalf of, and the number of warrants issued to, law enforcement officers of the agency during that year; and

(aa) the number of international assistance applications made by or on behalf of, and the number of warrants issued as a result of such applications to, law enforcement officers of the agency during that year; and

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

(c) the number of applications for tracking device authorisations made by, and the number of such authorisations given to, law enforcement officers of the agency during that year; and

(d) the number of remote applications for warrants made by or on behalf of law enforcement officers of the agency during that year; and

(e) the number of applications for warrants, emergency authorisations or tracking device authorisations made by or on behalf of law enforcement officers of the agency that were refused during that year, and the reasons for refusal; and

(ea) the number of international assistance applications made by or on behalf of law enforcement officers of the agency that were refused during that year, and the reasons for refusal; and

(eb) if the agency is the Australian Federal Police or the Australian Crime Commission—the kinds of offences targeted by data disruption warrants issued during that year in response to applications made by or on behalf of law enforcement officers of the agency; and

(ec) if the agency is the Australian Federal Police or the Australian Crime Commission—the kinds of offences in relation to which information was obtained under network

Authorised Version C2025C00651 registered 28/11/2025

activity warrants issued during that year in response to applications made by the chief officer of the agency; and

(f) the number of applications for extensions of warrants made by or on behalf of law enforcement officers of the agency during that year, the number of extensions granted or refused and the reasons why they were granted or refused; and

(g) the number of arrests made by law enforcement officers of the agency during that year on the basis (wholly or partly) of information obtained by:

(i) the use of a surveillance device under a warrant; or

(ii) access under a warrant to data held in a computer; or

(iii) an emergency authorisation for the use of a surveillance device; or

(iv) an emergency authorisation for access to data held in a computer; or

(v) a tracking device authorisation; and

(h) the number of instances during that year in which the location and safe recovery of children to whom recovery orders related was assisted (wholly or partly) by information obtained by:

(i) the use of a surveillance device under a warrant; or

(ii) access under a warrant to data held in a computer; or

(iii) an emergency authorisation for the use of a surveillance device; or

(iv) an emergency authorisation for access to data held in a computer; or

(v) a tracking device authorisation; and

(i) the number of prosecutions for relevant offences that were commenced during that year in which information obtained by:

(i) the use of a surveillance device under a warrant; or

(ii) access under a warrant to data held in a computer; or

(iii) an emergency authorisation for the use of a surveillance device; or

Authorised Version C2025C00651 registered 28/11/2025

(iv) an emergency authorisation for access to data held in a computer; or

(v) a tracking device authorisation;

was given in evidence and the number of those prosecutions in which a person was found guilty; and

(ia) for each of the following offences:

(i) an offence against a law of a foreign country;

(ii) a crime within the jurisdiction of the ICC (within the meaning of the *International Criminal Court Act 2002*);

(iii) a Tribunal offence (within the meaning of the *International War Crimes Tribunals Act 1995*);

in respect of which a warrant was issued as a result of an international assistance application made by or on behalf of law enforcement officers of the agency during the year—the offence (if any), under a law of the Commonwealth, a State or a Territory, that is of the same, or a substantially similar, nature; and

(j) any other information relating to the use of surveillance devices, access to data held in computers and the administration of this Act that the Minister considers appropriate.

(2) The information referred to in paragraphs (1)(a), (b) and (c) must be presented in such a way as to identify the number of warrants issued, emergency authorisations given, and tracking device authorisations given, in respect of each different kind of surveillance device.

(3) The report must be submitted 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 cause a copy of the report to be laid before each House of the Parliament within 15 sitting days of that House after the Minister receives it.

(5) Subsection (4) has effect subject to section 50A.

Authorised Version C2025C00651 registered 28/11/2025

50A Deferral of inclusion of information in annual report

Scope

(1) This section applies to information in a report submitted to the Minister under subsection 50(1) by the chief officer of a law enforcement agency.

Exclusion of information

(2) If the chief officer is satisfied that the information is Part 5.3 information or Part 9.10 information, the chief officer must advise the Minister in writing to exclude the information from the report before tabling it in Parliament under subsection 50(4).

(3) If the Minister is satisfied, on the advice of the chief officer, that the information is Part 5.3 information or Part 9.10 information, the Minister must:

(a) notify the chief officer in writing; and

(b) exclude the information from the report before tabling it in Parliament.

Inclusion of information in subsequent report

(4) If:

(a) because of subsection (3), the information has not been included in a report tabled in Parliament; and

(b) the chief officer submits a report (the ***later report***) to the Minister under subsection 50(1);

the chief officer must, before the Minister tables the later report:

(c) reconsider whether the information is Part 5.3 information or Part 9.10 information; and

(d) if the chief officer is satisfied that the information is not Part 5.3 information or Part 9.10 information—advise the Minister in writing to include the information in the later report before tabling it in Parliament.

Authorised Version C2025C00651 registered 28/11/2025

(5) If the Minister is satisfied, on the advice of the chief officer, that the information is not Part 5.3 information or Part 9.10 information, the Minister must:

(a) notify the chief officer in writing; and

(b) include the information in the later report before tabling it in Parliament.

Definitions

(6) In this section:

Part 5.3 information means information that, if made public, could reasonably be expected to enable a reasonable person to conclude that:

(a) a surveillance device warrant issued in response to an application under subsection 14(3BA) or (3C) authorising:

(i) the use of a surveillance device on particular premises; or

(ii) the use of a surveillance device in or on a particular object or class of object; or

(iii) the use of a surveillance device in respect of the conversations, activities or location of a particular person;

is likely to be, or is not likely to be, in force; or

(b) a computer access warrant issued in response to an application under subsection 27A(5A) or (6) authorising:

(i) access to data held in a particular computer; or

(ii) access to data held in a computer on particular premises; or

(iii) access to data held in a computer associated with, used by or likely to be used by, a particular person;

is likely to be, or is not likely to be, in force.

Part 9.10 information means information that, if made public, could reasonably be expected to enable a reasonable person to conclude that:

Authorised Version C2025C00651 registered 28/11/2025

(a) a surveillance device warrant issued in response to an application under subsection 14(3D) or (3E) authorising:
  (i) the use of a surveillance device on particular premises; or
  (ii) the use of a surveillance device in or on a particular object or class of object; or
  (iii) the use of a surveillance device in respect of the conversations, activities or location of a particular person;
  is likely to be, or is not likely to be, in force; or
(b) a computer access warrant issued in response to an application under subsection 27A(5B) or (6A) authorising:
  (i) access to data held in a particular computer; or
  (ii) access to data held in a computer on particular premises; or
  (iii) access to data held in a computer associated with, used by or likely to be used by, a particular person;
  is likely to be, or is not likely to be, in force.

51 Keeping documents connected with warrants, emergency authorisations and tracking device 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 instrument of revocation given to the chief officer under subsection 20(4), 27(4), 27G(4), 27KG(4) or 27KR(4);
(c) each record made under section 31 in relation to an emergency authorisation given to a law enforcement officer of the agency;
(d) each record made under section 40 in relation to a tracking device authorisation given to a law enforcement officer of the agency;
(e) each written application for an emergency authorisation made by a law enforcement officer of the agency;

Authorised Version C2025C00651 registered 28/11/2025

(f) each written application for a tracking device authorisation made by a law enforcement officer of the agency;

(g) a copy of each application made by or on behalf of a law enforcement officer of the agency for:

(i) a warrant; or

(ii) extension or variation of a warrant;

(h) a copy of each application made under section 33 by or on behalf of an appropriate authorising officer for approval of the giving of an emergency authorisation to a law enforcement officer of the agency;

(j) a copy of each report made to the Minister under section 49;

(k) a copy of each certificate issued by an appropriate authorising officer of the agency concerned under section 62;

(l) a copy of each advice the chief officer gives the Minister under subsection 50A(2) or paragraph 50A(4)(d);

(m) each notice the chief officer receives from the Minister under paragraph 50A(3)(a) or (5)(a).

52 Other records to be kept

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

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

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

(c) a statement as to whether each application made by or on behalf of an appropriate authorising officer for approval of the giving of an emergency authorisation to a law enforcement officer of the agency was granted, refused or withdrawn;

Authorised Version C2025C00651 registered 28/11/2025

(d) a statement as to whether each application made by a law enforcement officer of the agency for a tracking device authorisation was granted, refused or withdrawn;

(e) details of each use by the agency, or by a law enforcement officer of the agency, of information obtained by:

(i) the use of a surveillance device by a law enforcement officer of the agency; or

(ii) access, by a law enforcement officer of the agency, to data held in a computer;

(f) 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:

(i) the use of a surveillance device by a law enforcement officer of the agency; or

(ii) access, by a law enforcement officer of the agency, to data held in a computer;

(g) details of each occasion when, to the knowledge of a law enforcement officer of the agency, information obtained by:

(i) the use of a surveillance device by a law enforcement officer of the agency; or

(ii) access, by a law enforcement officer of the agency, to data held in a computer;

was given in evidence in a relevant proceeding;

(h) details of each occasion when, to the knowledge of a law enforcement officer of the agency, information obtained by:

(i) the use of a surveillance device by a law enforcement officer of the agency; or

(ii) access, by a law enforcement officer of the agency, to data held in a computer;

was used in the location and safe recovery of a child to whom a recovery order related;

(ha) if the agency is the Australian Federal Police or the Australian Crime Commission—details of things done under subsection 27KP(8) in relation to a network activity warrant;

Authorised Version C2025C00651 registered 28/11/2025

(j) details of the destruction of records or reports under paragraph 46(1)(b) or 46AA(1)(b) or subsection 46A(1) or (1A) or 46B(1) or (2);

(k) details of each reconsideration by the chief officer under paragraph 50A(4)(c) that does not result in the chief officer giving advice under paragraph 50A(4)(d).

(2) An instrument recording a matter for the purposes of subsection (1) is not a legislative instrument.

53 Register of warrants, emergency authorisations and tracking device authorisations

(1) The chief officer of a law enforcement agency must cause a register of warrants, emergency authorisations and tracking device authorisations sought by law enforcement officers of that agency to be kept.

(2) The register is to specify, for each warrant sought by or on behalf of a law enforcement officer of the agency:

(a) the date the warrant was issued or refused; and

(b) the name of the eligible Judge or nominated ART member who issued or refused to issue the warrant; and

(c) if the warrant was issued:

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

(ii) if the warrant was issued in relation to a relevant offence—the relevant offence in relation to which the warrant was issued; and

(iii) if the warrant was issued in relation to a recovery order—the date of issue of the recovery order and the name of the child to whom the order related; and

(iiia) if the warrant was issued in relation to an international assistance authorisation—each offence to which the authorisation relates; and

Authorised Version C2025C00651 registered 28/11/2025

(iiib) if the warrant was issued for the purposes of an integrity operation—details identifying the integrity authority for the operation and the relevant offence in respect of which the integrity authority was granted; and

(iiic) if the warrant is a surveillance device warrant or computer access warrant issued on the basis of a Part 5.3 supervisory order, or a community safety supervision order, that was in force—the date the order was made; and

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

(v) details of any variation or extension of the warrant.

(3) The register is to specify, for each emergency authorisation sought by a law enforcement officer of the agency:

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

(b) the name of the appropriate authorising officer who gave or refused to give the emergency authorisation; and

(c) if the emergency authorisation was given:

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

(ii) if the authorisation related to a relevant offence—the relevant offence in relation to which it was given; and

(iii) if the authorisation related to a recovery order—the date of issue of the recovery order and the name of the child to whom the order related; and

(iv) the date on which the application for approval of powers exercised under the authorisation was made; and

(v) whether that application for approval of powers exercised under the authorisation was successful or not.

(4) The register is to specify, for each tracking device authorisation sought by a law enforcement officer of the agency:

(a) the date the tracking device authorisation was given or refused; and

(b) the name of the appropriate authorising officer who gave or refused to give the tracking device authorisation; and

Authorised Version C2025C00651 registered 28/11/2025

(c) if the tracking device authorisation was given:

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

(ii) if the authorisation related to a relevant offence—the relevant offence in relation to which it was given; and

(iii) if the authorisation related to a recovery order—the date of issue of the recovery order and the name of the child to whom the order related; and

(iv) if the authorisation was given for the purposes of an integrity operation—details identifying the integrity authority authorising the operation and the relevant offence in respect of which the integrity authority was granted.

(5) The register is not a legislative instrument.

Authorised Version C2025C00651 registered 28/11/2025

Division 3—Inspections

54 Appointment of inspecting officers

The Ombudsman may, by appointment in writing, under this Division, appoint members of the Ombudsman's staff to be inspecting officers.

55 Inspection of records

(1) The Ombudsman must 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.

(1A) Subsection (1) does not apply to compliance with:

(a) Division 6 of Part 2 (network activity warrants); or

(b) the remaining provisions of this Act so far as they relate to network activity warrants.

(2) In the case of the Australian Crime Commission, the Ombudsman must also inspect the records of the Commission to determine the extent of compliance by the Commission with the surveillance device laws of any State or Territory in relation to any warrants or emergency authorisations sought, and surveillance devices used, by law enforcement officers of the Commission under those laws.

(2A) The Ombudsman may inspect the records of a law enforcement agency to determine the extent of compliance during any period with the conditions and provisions mentioned in subsection 49A(2) (about Part 5.3 warrants or Part 9.10 warrants) by the agency and law enforcement officers of the agency if:

(a) the chief officer of the agency notifies the Ombudsman under that subsection of a contravention of those conditions or provisions; and

(b) the contravention occurred in that period.

(2B) If:

Authorised Version C2025C00651 registered 28/11/2025

(a) the performance of a function, or the exercise of a power, conferred by Part 15 of the *Telecommunications Act 1997* is in connection with a warrant; and

(b) a law enforcement agency has records that relate to the performance of that function or the exercise of that power;

the Ombudsman may inspect those records in order to determine the extent of compliance with Part 15 of the *Telecommunications Act 1997* by the agency and law enforcement officers of the agency.

(3) For the purpose of an inspection under this section, the Ombudsman:

(a) after notifying the chief officer of the 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) despite any other law, is entitled to make copies of, and to take extracts from, records of the agency; and

(d) 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.

(4) 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 perform functions under this section.

(5) While an operation is being conducted under a warrant, emergency authorisation or tracking device authorisation, the Ombudsman may refrain from inspecting any records of the agency concerned that are relevant to the obtaining or execution of that warrant or authorisation.

Authorised Version C2025C00651 registered 28/11/2025

56 Power to obtain relevant information

(1) If the Ombudsman has reasonable grounds to believe that a law enforcement officer of a particular law enforcement agency is able to give information relevant to an inspection under this Division of the agency's records, subsections (2) and (3) have effect.

(2) The Ombudsman may, by writing given to the law enforcement officer, require the officer to give the information to the Ombudsman:

(a) by writing signed by the officer; and

(b) at a specified place and within a specified period.

(3) The Ombudsman may, by writing given to the law enforcement officer, require the officer to attend:

(a) before a specified inspecting officer; and

(b) at a specified place; and

(c) within a specified period or at a specified time on a specified day;

to answer questions relevant to the inspection.

(4) If the Ombudsman:

(a) has reasonable grounds to believe that a law enforcement officer of a particular law enforcement agency is able to give information relevant to an inspection under this Division of the agency's records; and

(b) does not know the officer's identity;

the Ombudsman may, by writing given to the chief officer of the agency, require the chief officer, or a person nominated by the chief officer, to attend:

(c) before a specified inspecting officer; and

(d) at a specified place; and

(e) within a specified period or at a specified time on a specified day;

to answer questions relevant to the inspection.

Authorised Version C2025C00651 registered 28/11/2025

(5) The place, and the period or the time and day, specified in a requirement under this section, must be reasonable having regard to the circumstances in which the requirement is made.

(6) A person must not refuse:
  (a) to attend before a person; or
  (b) to give information; or
  (c) to answer questions;
when required to do so under this section.

Penalty for an offence against this subsection: Imprisonment for 6 months.

57 Ombudsman to be given information and access despite other laws

(1) Despite any other law, a person is not excused from giving information, answering a question, or giving access to a document, as and when required under this Division, on the ground that giving the information, answering the question, or giving access to the document, as the case may be, would contravene a law, would be contrary to the public interest or might tend to incriminate the person or make the person liable to a penalty, but:
  (a) the information, the answer, or the fact that the person has given access to the document, as the case may be; and
  (b) any information or thing (including a document) obtained as a direct or indirect consequence of giving the information, answering the question or giving access to the document;
is not admissible in evidence against the person except in a proceeding by way of a prosecution for an offence against section 45 or against Part 7.4 or 7.7 of the *Criminal Code*.

(2) Nothing in section 45 or any other law prevents an officer of an agency from:
  (a) giving information to an inspecting officer (whether orally or in writing and whether or not in answer to a question); or

Authorised Version C2025C00651 registered 28/11/2025

(b) giving access to a record of the agency to an inspecting officer;

for the purposes of an inspection under this Division of the agency's records.

(3) Nothing in section 45 or any other law prevents an officer of an agency from making a record of information, or causing a record of information to be made, for the purposes of giving the information to a person as permitted by subsection (2).

58 Exchange of information between Ombudsman and State inspecting authorities

(1) In this section:

State or Territory agency means a law enforcement agency of a State or Territory within the meaning of the law of that State or Territory that is of a similar nature to this Act.

State or Territory inspecting authority, in relation to a State or Territory agency, means the authority that, under the law of the State or Territory concerned, has the function of making inspections of a similar kind to those provided for in section 55 when the State or Territory agency is exercising powers under the law of that State or Territory that is of a similar nature to this Act.

(2) The Ombudsman may give information that:

(a) relates to a State or Territory agency; and

(b) was obtained by the Ombudsman under this Act;

to the State or Territory inspecting authority in relation to the agency.

(3) The Ombudsman may only give information to an authority under subsection (2) if the Ombudsman is satisfied that the giving of the information is necessary to enable the authority to perform its functions in relation to the State or Territory agency.

Authorised Version C2025C00651 registered 28/11/2025

(4) The Ombudsman may receive from a State or Territory inspecting authority information relevant to the performance of the Ombudsman's functions under this Act.

59 Delegation by Ombudsman

(1) The Ombudsman may delegate:

(a) to an APS employee responsible to the Ombudsman; or

(b) to a person having similar oversight functions to the Ombudsman under the law of a State or Territory or to an employee responsible to that person;

all or any of the Ombudsman's powers under this Division other than a power to report to the Minister.

(2) A delegate must, upon request by a person affected by the exercise of any power delegated to the delegate, produce the instrument of delegation, or a copy of the instrument, for inspection by the person.

60 Ombudsman not to be sued

The Ombudsman, an inspecting officer, or a person acting under an inspecting officer's direction or authority, is not liable to an action, suit or proceeding for or in relation to an act done, or omitted to be done, in good faith in the performance or exercise, or the purported performance or exercise, of a function or power conferred by this Division.

61 Report on inspection

(1) The Ombudsman must make a written report to the Minister at 6 monthly intervals on the results of each inspection under section 55.

(2) The Minister must cause a copy of the report to be laid before each House of the Parliament within 15 sitting days of that House after the Minister receives it.

Authorised Version C2025C00651 registered 28/11/2025

(3) If the report relates, in whole or in part, to an inspection under section 55 of compliance by the Australian Crime Commission with the surveillance device laws of a State or Territory, the Minister must, as soon as practicable after the report is laid before each House of the Parliament, send a copy of the report to the Minister of that State or Territory with responsibility for the surveillance device laws of that State or Territory.

Part 5.3 information or Part 9.10 information

(4) The Minister must exclude information from the report before the Minister causes a copy of the report to be laid before each House of the Parliament if the Minister is satisfied that the information is Part 5.3 information or Part 9.10 information.

(5) If the Minister must send a copy of the report to a Minister of a State under subsection (3), subsection (4) does not require the Minister to exclude from that copy information that the Minister must exclude from the copy of the report the Minister causes to be laid before each House of the Parliament.

(6) If:

(a) because of subsection (4), information has not been included in a copy of a report laid before each House of the Parliament under subsection (2); and

(b) the Ombudsman makes a report (the ***later report***) to the Minister under subsection (1);

the Minister must, before causing a copy of the later report to be laid before each House of the Parliament:

(c) reconsider whether the information is Part 5.3 information or Part 9.10 information; and

(d) if the Minister is satisfied that the information is not Part 5.3 information or Part 9.10 information—include the information in the copy of the later report before causing it to be laid before each House of the Parliament under subsection (2).

Authorised Version C2025C00651 registered 28/11/2025

61A Report may cover notified breaches in relation to Part 5.3 warrants or Part 9.10 warrants

(1) In a report under subsection 61(1) in relation to a 6-month period, the Ombudsman may include a report on a contravention of which the Ombudsman is notified under subsection 49A(2) (about Part 5.3 warrants or Part 9.10 warrants), if the Ombudsman does not conduct an inspection under subsection 55(2A) in relation to a period during which the contravention occurred.

Note: If the Ombudsman conducts an inspection under subsection 55(2A), the Ombudsman must report on the results of the inspection under subsection 61(1).

(2) For the purposes of subsection (1), it does not matter whether the Ombudsman is notified under subsection 49A(2) before, during or after the 6-month period to which the report relates.

(3) Subsection (1) does not limit what the Ombudsman may include in a report under section 61.

Authorised Version C2025C00651 registered 28/11/2025

Division 4—General

62 Evidentiary certificates

(1) An appropriate authorising officer for a law enforcement officer, or a person assisting the appropriate authorising officer, may issue a written certificate signed by the officer or person, setting out any facts he or she considers relevant with respect to:

(a) anything done by the law enforcement officer or by a person assisting or providing technical expertise to him or her:

(i) in connection with the execution of a warrant; or

(ii) in accordance with an emergency authorisation; or

(iii) in accordance with a tracking device authorisation; or

(b) anything done by the law enforcement officer in connection with:

(i) the communication by a person to another person; 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 or tracking device authorisation; or

(c) anything done by the law enforcement officer in connection with:

(i) the communication by a person to another person; or

(ii) the making use of; or

(iii) the making of a record of; or

(iv) the custody of a record of;

information obtained from access to data under:

(v) a computer access warrant; or

(vi) an emergency authorisation for access to data held in a computer; or

(d) anything done by the law enforcement officer in connection with:

Authorised Version C2025C00651 registered 28/11/2025

(i) the communication by a person to another person 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 from access to, or disruption of, data under:

(v) a data disruption warrant; or
(vi) an emergency authorisation for disruption of data held in a computer; or

(e) anything done by the law enforcement officer in connection with:

(i) the communication by a person to another person; or
(ii) the making use of; or
(iii) the making of a record of; or
(iv) the custody of a record of;

information obtained from access to data under a network activity warrant.

(2) A certificate issued under subsection (1) is admissible in evidence in any proceedings as prima facie evidence of the matters stated in the certificate.

(3) Subsection (2) does not apply to a certificate to the extent that the certificate sets out facts with respect to anything done in accordance with an emergency authorisation unless the giving of that authorisation has been approved under section 35, 35A or 35B.

(4) For the purposes of this section, a document purporting to be a certificate issued under subsection (1) is, unless the contrary intention is established, to be taken to be such a certificate and to have been duly given.

(5) A certificate must not be admitted in evidence under subsection (2) in prosecution proceedings unless the person charged or a solicitor who has appeared for the person in those proceedings has, at least 14 days before the certificate is sought to be so admitted, been given a copy of the certificate together with reasonable evidence of

Authorised Version C2025C00651 registered 28/11/2025

the intention to produce the certificate as evidence in those proceedings.

(6) Subject to subsection (7), if, under subsection (2), a certificate is admitted in evidence in prosecution proceedings, the person charged may require the person giving the certificate to be called as a witness for the prosecution and cross-examined as if he or she had given evidence of the matters stated in the certificate.

(7) Subsection (6) does not entitle the person charged to require the person giving a certificate to be called as a witness for the prosecution unless the court before which the prosecution proceedings are brought, by order, allows the person charged to require the person giving the certificate to be so called.

(8) Any evidence given in support, or in rebuttal, of a matter stated in a certificate given under subsection (2) or (3) must be considered on its merits and the credibility and probative value of such evidence must be neither increased nor diminished by reason of this section.

Authorised Version C2025C00651 registered 28/11/2025

Part 7—Miscellaneous

63 Delegation by chief officer of law enforcement agency

The chief officer of a law enforcement agency may, by writing, delegate to a member of the staff of the agency who is an SES employee or a person of equivalent rank, all or any of the chief officer's powers or functions.

64 Compensation for loss or injury

(1) If:

(a) a person suffers loss or injury as a result of the use of a surveillance device by any of the following:

(i) the Australian Federal Police;

(ii) the National Anti-Corruption Commissioner or another National Anti-Corruption Commission officer;

(iii) the Australian Crime Commission; and

(b) the use of that device:

(i) is prohibited by the law of the State or Territory in which the use occurs; and

(ii) is not in accordance with this Act;

the Commonwealth is liable to pay to the person who has suffered the loss or injury such compensation as is agreed on between the Commonwealth and that person or, in default of such an agreement, as is determined by action against the Commonwealth in a court of competent jurisdiction.

(2) If:

(a) a person suffers loss or injury as a result of the use of:

(i) a computer; or

(ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or

(iii) any other electronic equipment; or

Authorised Version C2025C00651 registered 28/11/2025

(iv) a data storage device;

for the purpose of obtaining access to, or disrupting, data that is held in the computer; and

(b) the use of the computer, facility, equipment or device, as the case may be, was by any of the following:

(i) the Australian Federal Police;

(ii) the National Anti-Corruption Commissioner or another National Anti-Corruption Commission officer;

(iii) the Australian Crime Commission; and

(c) the use of the computer, facility, equipment or device, as the case may be, is prohibited by the law of the State or Territory in which the use occurs; and

(d) the use of the computer, facility, equipment or device, as the case may be, is neither:

(i) in accordance with this Act; nor

(ii) in the performance of a function, or the exercise of a power, conferred by a law of the Commonwealth;

the Commonwealth is liable to pay to the person who has suffered the loss or injury:

(e) such compensation as is agreed on between the Commonwealth and that person; or

(f) in default of such an agreement—such compensation as is determined by action against the Commonwealth in a court of a State or Territory that has jurisdiction in relation to the matter.

(3) If:

(a) a person suffers loss or injury as a result of the use of:

(i) a computer; or

(ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or

(iii) any other electronic equipment; or

(iv) a data storage device;

for the purpose of obtaining access to, or disrupting, data that is held in the computer; and

Authorised Version C2025C00651 registered 28/11/2025

(b) the use of the computer, facility, equipment or device, as the case may be, was authorised by an emergency authorisation for disruption of data held in a computer; and

(c) the giving of the emergency authorisation was not approved under section 35B;

the Commonwealth is liable to pay to the person who has suffered the loss or injury:

(d) such compensation as is agreed on between the Commonwealth and that person; or

(e) in default of such an agreement—such compensation as is determined by action against the Commonwealth in a court of a State or Territory that has jurisdiction in relation to the matter.

64A Person with knowledge of a computer or a computer system to assist access etc.

(1) A law enforcement officer (or another person on the officer's behalf) may apply for an order (the ***assistance order***) requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to do one or more of the following:

(a) access data held in a computer that is the subject of:

(i) a computer access warrant; or

(ia) a network activity warrant; or

(ii) an emergency authorisation given in response to an application under subsection 28(1A), 29(1A) or 30(1A);

(b) copy data held in the computer described in paragraph (a) to a data storage device;

(c) convert into documentary form or another form intelligible to a law enforcement officer:

(i) data held in the computer described in paragraph (a); or

(ii) data held in a data storage device to which the data was copied as described in paragraph (b).

(1A) The application may be made to:

Authorised Version C2025C00651 registered 28/11/2025

(a) for an application made by a law enforcement officer of the National Anti-Corruption Commission—an eligible Judge; or

(b) otherwise—an eligible Judge or a nominated ART member.

Warrants and emergency authorisations relating to relevant offences

(2) In the case of a computer that is the subject of:

(a) a computer access warrant issued in relation to a relevant offence; or

(b) an emergency authorisation given in response to an application under subsection 28(1A);

the eligible Judge or nominated ART member may grant the assistance order if the eligible Judge or nominated ART member is satisfied that:

(c) there are reasonable grounds for suspecting that access to data held in the computer is necessary in the course of the investigation for the purpose of enabling evidence to be obtained of:

(i) the commission of those offences; or

(ii) the identity or location of the offenders; and

(d) the specified person is:

(i) reasonably suspected of having committed any of the offences to which the warrant or emergency authorisation relates; or

(ii) the owner or lessee of the computer or device; or

(iii) an employee of the owner or lessee of the computer or device; or

(iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or

(v) a person who uses or has used the computer or device; or

(vi) a person who is or was a system administrator for the system including the computer or device; and

(e) the specified person has relevant knowledge of:

Authorised Version C2025C00651 registered 28/11/2025

(i) the computer or device or a computer network of which the computer or device forms or formed a part; or

(ii) measures applied to protect data held in the computer or device.

Warrants and emergency authorisations relating to recovery orders

(3) In the case of a computer that is the subject of:

(a) a computer access warrant issued in relation to a recovery order; or

(b) an emergency authorisation given in response to an application under subsection 29(1A);

the eligible Judge or nominated ART member may grant the assistance order if the eligible Judge or nominated ART member is satisfied that:

(c) there are reasonable grounds for suspecting that access to data held in the computer may assist in the location and safe recovery of the child to whom the recovery order relates; and

(d) the specified person is:

(i) the owner or lessee of the computer; or

(ii) an employee of the owner or lessee of the computer; or

(iii) a person engaged under a contract for services by the owner or lessee of the computer; or

(iv) a person who uses or has used the computer; or

(v) a person who is or was a system administrator for the system including the computer; and

(e) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer.

Warrants relating to international assistance authorisations

(4) In the case of a computer that is the subject of a computer access warrant issued in relation to an international assistance

Authorised Version C2025C00651 registered 28/11/2025

authorisation, the eligible Judge or nominated ART member may grant the assistance order if the eligible Judge or nominated ART member is satisfied that:

(a) there are reasonable grounds for suspecting that access to data held in the computer is necessary, in the course of the investigation or investigative proceeding to which the authorisation relates, for the purpose of enabling evidence to be obtained of:

(i) the commission of an offence to which the authorisation relates; or

(ii) the identity or location of the persons suspected of committing the offence; and

(b) the specified person is:

(i) reasonably suspected of committing an offence to which the authorisation relates; or

(ii) the owner or lessee of the computer; or

(iii) an employee of the owner or lessee of the computer; or

(iv) a person engaged under a contract for services by the owner or lessee of the computer; or

(v) a person who uses or has used the computer; or

(vi) a person who is or was a system administrator for the system including the computer; and

(c) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer.

Warrants relating to integrity operations

(5) In the case of a computer that is the subject of a computer access warrant issued in relation to an integrity operation, the eligible Judge or nominated ART member may grant the assistance order if the eligible Judge or nominated ART member is satisfied that:

(a) there are reasonable grounds for suspecting that access to data held in the computer will assist the conduct of the integrity operation by enabling evidence to be obtained

Authorised Version C2025C00651 registered 28/11/2025

relating to the integrity, location or identity of a particular staff member of the target agency; and

(b) the specified person is:

(i) the staff member; or

(ii) the owner or lessee of the computer; or

(iii) an employee of the owner or lessee of the computer; or

(iv) a person engaged under a contract for services by the owner or lessee of the computer; or

(v) a person who uses or has used the computer; or

(vi) a person who is or was a system administrator for the system including the computer; and

(c) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer.

Part 5.3 warrants

(6) In the case of a computer that is subject to a Part 5.3 warrant that is a computer access warrant, the eligible Judge or nominated ART member may grant the assistance order if the eligible Judge or nominated ART member is satisfied that:

(a) there are reasonable grounds for suspecting that access to the data held in the computer would be likely to substantially assist in:

(i) if the computer access warrant was issued to determine whether to apply for a post-sentence order—determining whether to apply for the post-sentence order; or

(ii) if the computer access warrant was issued on the basis of a Part 5.3 supervisory order that is in force—achieving a Part 5.3 object, or determining whether the Part 5.3 supervisory order, or any succeeding Part 5.3 supervisory order, has been, or is being, complied with; and

(b) the specified person is:

Authorised Version C2025C00651 registered 28/11/2025

(ia) if the warrant was issued to determine whether to apply for a post-sentence order—the person to whom the application relates; or

(i) if the warrant was issued in relation to a Part 5.3 supervisory order that is in force—the subject of the Part 5.3 supervisory order; or

(ii) the owner or lessee of the computer; or

(iii) an employee of the owner or lessee of the computer; or

(iv) a person engaged under a contract for services by the owner or lessee of the computer; or

(v) a person who uses or has used the computer; or

(vi) a person who is or was a system administrator for the system including the computer; and

(c) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer.

Part 9.10 warrants

(6AA) In the case of a computer that is subject to a Part 9.10 warrant that is a computer access warrant, the eligible Judge or nominated ART member may grant the assistance order if the eligible Judge or nominated ART member is satisfied that:

(a) there are reasonable grounds for suspecting that access to the data held in the computer would be likely to substantially assist in:

(i) if the computer access warrant was issued to determine whether to apply for a Part 9.10 order—determining whether to apply for the Part 9.10 order; or

(ii) if the computer access warrant was issued on the basis of a community safety supervision order that is in force—achieving a Part 9.10 object, or determining whether the community safety supervision order, or any succeeding community safety supervision order, has been, or is being, complied with; and

Authorised Version C2025C00651 registered 28/11/2025

(b) the specified person is:

(i) if the warrant was issued to determine whether to apply for a Part 9.10 order—the person to whom the application relates; or

(ii) if the warrant was issued in relation to a community safety supervision order that is in force—the subject of the community safety supervision order; or

(iii) the owner or lessee of the computer; or

(iv) an employee of the owner or lessee of the computer; or

(v) a person engaged under a contract for services by the owner or lessee of the computer; or

(vi) a person who uses or has used the computer; or

(vii) a person who is or was a system administrator for the system including the computer; and

(c) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer.

Network activity warrant

(6A) In the case of a computer that is the subject of a network activity warrant, the eligible Judge or nominated ART member may grant the assistance order if the eligible Judge or nominated ART member is satisfied that:

(a) there are reasonable grounds for suspecting that access to data held in the computer will substantially assist in the collection of intelligence that:

(i) relates to the group referred to in paragraph 27KK(1)(a) or to any of the individuals in the group; and

(ii) is relevant to the prevention, detection or frustration of one or more kinds of relevant offences; and

(b) the specified person is:

(i) reasonably suspected of having committed any of the relevant offences in respect of which the warrant was issued; or

Authorised Version C2025C00651 registered 28/11/2025

(ii) the owner or lessee of the computer; or

(iii) an employee of the owner or lessee of the computer; or

(iv) a person engaged under a contract for services by the owner or lessee of the computer; or

(v) a person who uses or has used the computer; or

(vi) a person who is or was a system administrator for the system including the computer; and

(c) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer.

Emergency authorisations relating to risk of loss of evidence

(7) In the case of a computer that is the subject of an emergency authorisation given in response to an application under subsection 30(1A), the eligible Judge or nominated ART member may grant the assistance order if the eligible Judge or nominated ART member is satisfied that:

(a) there are reasonable grounds for suspecting that access to data held in the computer is necessary to prevent the loss of any evidence relevant to the investigation to which the subsection 30(1A) application relates; and

(b) the specified person is:

(i) reasonably suspected of having committed any of the offences to which the emergency authorisation relates; or

(ii) the owner or lessee of the computer or device; or

(iii) an employee of the owner or lessee of the computer or device; or

(iv) a person engaged under a contract for services by the owner or lessee of the computer or device; or

(v) a person who uses or has used the computer or device; or

(vi) a person who is or was a system administrator for the system including the computer or device; and

Authorised Version C2025C00651 registered 28/11/2025

(c) the specified person has relevant knowledge of:

(i) the computer or device or a computer network of which the computer or device forms or formed a part; or

(ii) measures applied to protect data held in the computer or device.

(7A) In determining whether the assistance order should be granted, the eligible Judge or nominated ART member must have regard to whether the specified person is, or has been, subject to:

(a) another order under this section; or

(b) an order under section 64B of this Act; or

(c) an order under section 3LA or 3ZZVG of the *Crimes Act 1914*;

so far as that matter is known to the eligible Judge or nominated ART member.

(7B) Subsection (7A) does not limit the matters to which the eligible Judge or nominated ART member may have regard.

Duration of assistance order

(7C) If an assistance order is granted in relation to a computer that is the subject of a computer access warrant or a network activity warrant, the order ceases to be in force when the warrant ceases to be in force.

(7D) If an assistance order is granted in relation to a computer that is the subject of an emergency authorisation given in response to an application under subsection 28(1A), 29(1A) or 30(1A), the order ceases to be in force when the emergency authorisation ceases to be in force.

Protection from civil liability

(7E) A person is not subject to any civil liability in respect of an act done by the person:

(a) in compliance with an assistance order; or

Authorised Version C2025C00651 registered 28/11/2025

(b) in good faith in purported compliance with an assistance order.

Offence

(8) A person commits an offence if:

(a) the person is subject to an order under this section; and

(b) the person is capable of complying with a requirement in the order; and

(c) the person omits to do an act; and

(d) the omission contravenes the requirement.

Penalty for contravention of this subsection: Imprisonment for 10 years or 600 penalty units, or both.

64B Person with knowledge of a computer or a computer system to assist disruption of data etc.

(1) A law enforcement officer of the Australian Federal Police or the Australian Crime Commission (or another person on the officer's behalf) may apply to an eligible Judge or to a nominated ART member for an order (the ***assistance order***) requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to do one or more of the following:

(a) disrupt data held in a computer that is the subject of:

(i) a data disruption warrant; or

(ii) an emergency authorisation given in response to an application under subsection 28(1C);

(b) access data that is held in the computer described in paragraph (a);

(c) copy data held in the computer described in paragraph (a) to a data storage device;

(d) convert into documentary form or another form intelligible to a law enforcement officer:

(i) data held in the computer described in paragraph (a); or

Authorised Version C2025C00651 registered 28/11/2025

(ii) data held in a data storage device to which the data was copied as described in paragraph (c).

Grant of assistance order

(2) The eligible Judge or nominated ART member may grant the assistance order if the eligible Judge or nominated ART member is satisfied that:

(a) in a case where the computer is the subject of a data disruption warrant—disruption of data held in the computer is:

(i) likely to substantially assist in frustrating the commission of the offences that are covered by the warrant (within the meaning of section 27KE); and

(ii) justifiable and proportionate, having regard to those offences; and

(aa) in a case where the computer is the subject of a data disruption warrant—the assistance order is reasonable and necessary to enable the warrant to be executed; and

(ab) in a case where the computer is the subject of a data disruption warrant—the assistance order is justifiable and proportionate, having regard to:

(i) the nature and gravity of the conduct constituting the offences referred to in paragraph 27KA(1)(c); and

(ii) the likely impact of compliance with the assistance order on the specified person, so far as that matter is known to the eligible Judge or nominated ART member; and

(iii) the likely impact of compliance with the assistance order on other persons (including persons who may lawfully be using the computer), so far as that matter is known to the eligible Judge or nominated ART member; and

(b) in a case where the computer is the subject of an emergency authorisation given in response to an application under subsection 28(1C):

Authorised Version C2025C00651 registered 28/11/2025

(i) there is an imminent risk of serious violence to a person or substantial damage to property; and

(ii) disruption of data held in the computer is immediately necessary for the purpose of dealing with the risk; and

(ba) in a case where the computer is the subject of an emergency authorisation given in response to an application under subsection 28(1C)—the assistance order is reasonable and necessary to enable the emergency authorisation to be executed; and

(bb) in a case where the computer is the subject of an emergency authorisation given in response to an application under subsection 28(1C)—the assistance order is justifiable and proportionate, having regard to:

(i) the risk of serious violence or substantial damage referred to in paragraph 28(1C)(a); and

(ii) the likely impact of compliance with the assistance order on the specified person, so far as that matter is known to the eligible Judge or nominated ART member; and

(iii) the likely impact of compliance with the assistance order on other persons (including persons who may lawfully be using the computer), so far as that matter is known to the eligible Judge or nominated ART member; and

(c) in a case where:

(i) the computer is the subject of a data disruption warrant; and

(ii) the assistance order requires the specified person to provide information or assistance to allow the law enforcement officer to do a thing referred to in paragraph (1)(b), (c) or (d) in relation to data;

doing the thing is for the purpose of determining whether the data is covered by the warrant (within the meaning of section 27KE); and

(d) in a case where:

Authorised Version C2025C00651 registered 28/11/2025

(i) the computer is the subject of an emergency authorisation given in response to an application under subsection 28(1C); and

(ii) the assistance order requires the specified person to provide information or assistance to allow the law enforcement officer to do a thing referred to in paragraph (1)(b), (c) or (d) in relation to data;

doing the thing is for the purpose of determining whether disruption of the data is immediately necessary for the purpose of dealing with an imminent risk of serious violence to a person or substantial damage to property; and

(e) the specified person is:

(i) in a case where the computer is the subject of a data disruption warrant—reasonably suspected of having committed any of the relevant offences referred to in paragraph 27KA(1)(c); or

(ii) in a case where the computer is the subject of emergency authorisation—reasonably suspected of having committed the relevant offence referred to in subsection 28(1C); or

(iii) the owner or lessee of the computer; or

(iv) an employee of the owner or lessee of the computer; or

(v) a person engaged under a contract for services by the owner or lessee of the computer; or

(vi) a person who uses or has used the computer; or

(vii) a person who is or was a system administrator for the system including the computer; and

(f) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer.

(2A) In determining whether the assistance order should be granted, the eligible Judge or nominated ART member must have regard to whether the specified person is, or has been, subject to:

(a) another order under this section; or

Authorised Version C2025C00651 registered 28/11/2025

(b) an order under section 64A of this Act; or

(c) an order under section 3LA or 3ZZVG of the *Crimes Act 1914*;

so far as that matter is known to the eligible Judge or nominated ART member.

(2B) Subsection (2A) does not limit the matters to which the eligible Judge or nominated ART member may have regard.

Duration of assistance order

(2C) If an assistance order is granted in relation to a computer that is the subject of a data disruption warrant, the order ceases to be in force when the warrant ceases to be in force.

(2D) If an assistance order is granted in relation to a computer that is the subject of an emergency authorisation given in response to an application under subsection 28(1C), the order ceases to be in force when the emergency authorisation ceases to be in force.

Protection from civil liability

(2E) A person is not subject to any civil liability in respect of an act done by the person:

(a) in compliance with an assistance order; or

(b) in good faith in purported compliance with an assistance order.

Offence

(3) A person commits an offence if:

(a) the person is subject to an order under this section; and

(b) the person is capable of complying with a requirement in the order; and

(c) the person omits to do an act; and

(d) the omission contravenes the requirement.

Penalty for contravention of this subsection: Imprisonment for 10 years or 600 penalty units, or both.

Authorised Version C2025C00651 registered 28/11/2025

65 Minor defects in connection with warrant or other authority

(1) If:

(a) information or a record is purportedly obtained through the use of a surveillance device authorised by a warrant, emergency authorisation or tracking device authorisation; and

(b) there is a defect or irregularity in relation to the warrant, emergency authorisation or tracking device authorisation; and

(c) but for that defect or irregularity, the warrant, emergency authorisation or tracking device authorisation would be a sufficient authority for the use of that surveillance device in obtaining that information or record;

then:

(d) the use of that device is to be treated as being as valid; and

(e) the information or record obtained through that use may be dealt with, or given in evidence in any proceeding;

as if the warrant, emergency authorisation or tracking device authorisation did not have that defect or irregularity.

(1A) If:

(a) information or a record is purportedly obtained through accessing, under a computer access warrant, data disruption warrant, network activity warrant or emergency authorisation, particular data held in a computer; and

(b) there is a defect or irregularity in relation to the warrant or emergency authorisation; and

(c) but for that defect or irregularity, the warrant or emergency authorisation would be a sufficient authority for accessing the data;

then:

(d) access to the data is taken to be as valid; and

(e) the information or record obtained through accessing the data may be dealt with, or given in evidence in any proceeding;

Authorised Version C2025C00651 registered 28/11/2025

as if the warrant or emergency authorisation did not have that defect or irregularity.

(1B) If:

(a) data is disrupted purportedly under:

(i) a data disruption warrant; or

(ii) an emergency authorisation for disruption of data held in a computer; and

(b) there is a defect or irregularity in relation to the warrant or emergency authorisation; and

(c) but for that defect or irregularity, the warrant or emergency authorisation would be a sufficient authority for disrupting the data;

disruption of the data is taken to be as valid as if the warrant or emergency authorisation did not have that defect or irregularity.

(2) A reference in subsection (1), (1A) or (1B) to a defect or irregularity in relation to the warrant, emergency authorisation or tracking device authorisation is a reference to a defect or irregularity (other than a substantial defect or irregularity):

(a) in, or in connection with the issue of, a document purporting to be that warrant, emergency authorisation or tracking device authorisation; or

(b) in connection with the execution of that warrant, emergency authorisation or tracking device authorisation, or the purported execution of a document purporting to be that warrant, emergency authorisation or tracking device authorisation.

65A Protection of persons—control order declared to be void

Surveillance device warrant issued for control order

(1) If:

(a) a surveillance device warrant was issued on the basis that an interim control order was in force; and

Authorised Version C2025C00651 registered 28/11/2025

(b) a court subsequently declares the interim control order to be void;

a criminal proceeding does not lie against a person in respect of anything done, or omitted to be done, in good faith by the person:

(c) in the purported execution of the warrant; or

(d) in the purported exercise of a power, or the purported performance of a function or duty, in a case where the purported exercise of the power, or the purported performance of the function or duty, is consequential on the warrant.

(2) Subsection (1) does not apply to a thing done, or omitted to be done, at a particular time if, at that time, the person knew, or ought reasonably to have known, of the declaration.

Computer access warrant issued for control order

(2A) If:

(a) a computer access warrant was issued on the basis that an interim control order was in force; and

(b) a court subsequently declares the interim control order to be void;

a criminal proceeding does not lie against a person in respect of anything done, or omitted to be done, in good faith by the person:

(c) in the purported execution of the warrant; or

(d) in the purported exercise of a power, or the purported performance of a function or duty, in a case where the purported exercise of the power, or the purported performance of the function or duty, is consequential on the warrant.

(2B) Subsection (2A) does not apply to a thing done, or omitted to be done, at a particular time if, at that time, the person knew, or ought reasonably to have known, of the declaration.

Tracking device authorisation

(3) If:

Authorised Version C2025C00651 registered 28/11/2025

(a) a tracking device authorisation was given on the basis that an interim control order was in force; and

(b) a court subsequently declares the interim control order to be void;

a criminal proceeding does not lie against a person in respect of anything done, or omitted to be done, in good faith by the person:

(c) in the purported execution of the authorisation; or

(d) in the purported exercise of a power, or the purported performance of a function or duty, in a case where the purported exercise of the power, or the purported performance of the function or duty, is consequential on the authorisation.

(4) Subsection (3) does not apply to a thing done, or omitted to be done, at a particular time if, at that time, the person knew, or ought reasonably to have known, of the declaration.

Use of device without warrant

(5) If:

(a) an optical surveillance device was used under subsection 37(4) on the basis that an interim control order was in force; and

(b) a court subsequently declares the interim control order to be void;

a criminal proceeding does not lie against a person in respect of anything done, or omitted to be done, in good faith by the person:

(c) in the purported exercise of the power conferred by subsection 37(4); or

(d) in the purported exercise of a power, or the purported performance of a function or duty, in a case where the purported exercise of the power, or the purported performance of the function or duty, is consequential on the purported exercise of the power conferred by subsection 37(4).

Authorised Version C2025C00651 registered 28/11/2025

(6) Subsection (5) does not apply to a thing done, or omitted to be done, at a particular time if, at that time, the person knew, or ought reasonably to have known, of the declaration.

(7) If:

(a) a surveillance device was used under subsection 38(3A) or (6) on the basis that an interim control order was in force; and

(b) a court subsequently declares the interim control order to be void;

a criminal proceeding does not lie against a person in respect of anything done, or omitted to be done, in good faith by the person:

(c) in the purported exercise of the power conferred by subsection 38(3A) or (6), as the case requires; or

(d) in the purported exercise of a power, or the purported performance of a function or duty, in a case where the purported exercise of the power, or the purported performance of the function or duty, is consequential on the purported exercise of the power conferred by subsection 38(3A) or (6), as the case requires.

(8) Subsection (7) does not apply to a thing done, or omitted to be done, at a particular time if, at that time, the person knew, or ought reasonably to have known, of the declaration.

65B Dealing with information obtained under a warrant or authorisation etc.—control order declared to be void

Scope

(1) This section applies if:

(a) any of the following conditions is satisfied:

(i) a surveillance device warrant was issued on the basis that an interim control order was in force;

(ia) a computer access warrant was issued on the basis that an interim control order was in force;

Authorised Version C2025C00651 registered 28/11/2025

(ii) a tracking device authorisation was given on the basis that an interim control order was in force;

(iii) an optical surveillance device was used under subsection 37(4) on the basis that an interim control order was in force;

(iv) a surveillance device was used under subsection 38(3A) or (6) on the basis that an interim control order was in force; and

(b) a court subsequently declares the interim control order to be void; and

(c) if subparagraph (a)(i) applies—before the declaration was made, information was obtained as a result of:

(i) the purported execution of the warrant; or

(ii) the purported exercise of a power, or the purported performance of a function or duty, in a case where the purported exercise of the power, or the purported performance of the function or duty, is consequential on the warrant; and

(d) if subparagraph (a)(ii) applies—before the declaration was made, information was obtained as a result of:

(i) the purported execution of the authorisation; or

(ii) the purported exercise of a power, or the purported performance of a function or duty, in a case where the purported exercise of the power, or the purported performance of the function or duty, is consequential on the authorisation; and

(e) if subparagraph (a)(iii) applies—before the declaration was made, information was obtained as a result of:

(i) the purported exercise of the power conferred by subsection 37(4); or

(ii) the purported exercise of a power, or the purported performance of a function or duty, in a case where the purported exercise of the power, or the purported performance of the function or duty, is consequential on the purported exercise of the power conferred by subsection 37(4); and

Authorised Version C2025C00651 registered 28/11/2025

(f) if subparagraph (a)(iv) applies—before the declaration was made, information was obtained as a result of:

(i) the purported exercise of the power conferred by subsection 38(3A) or (6), as the case requires; or

(ii) the purported exercise of a power, or the purported performance of a function or duty, in a case where the purported exercise of the power, or the purported performance of the function or duty, is consequential on the purported exercise of the power conferred by subsection 38(3A) or (6), as the case requires.

Dealing

(2) A person may use, communicate or publish the information if:

(a) the person reasonably believes that doing so is necessary to assist in preventing, or reducing the risk, of:

(i) the commission of a terrorist act; or

(ii) serious harm to a person; or

(iii) serious damage to property; or

(b) the person does so for one or more purposes set out in subsection (4).

Evidence

(3) The information may be admitted in evidence in any proceedings if:

(a) doing so is necessary to assist in preventing, or reducing the risk, of:

(i) the commission of a terrorist act; or

(ii) serious harm to a person; or

(iii) serious damage to property; or

(b) it is admitted for one or more purposes set out in subsection (4).

Authorised Version C2025C00651 registered 28/11/2025

Purposes

(4) The purposes are purposes connected with the performance of a function or duty, or the exercise of a power, by a person, court, tribunal or other body under, or in relation to a matter arising under, a preventative detention order law, so far as the function, duty or power relates to a preventative detention order (within the meaning of that preventative detention order law).

Definition

(5) In this section:

serious harm has the same meaning as in the *Criminal Code*.

65C Evidence obtained from access to, or disruption of, data under a data disruption warrant etc.

This Act does not prevent evidence obtained from access to, or disruption of, data under:

(a) a data disruption warrant; or

(b) an emergency authorisation for disruption of data held in a computer;

from being admissible as evidence in a proceeding relating to a relevant offence.

66 Regulations

(1) The Governor-General may make regulations prescribing matters:

(a) required or permitted by this Act to be prescribed; or

(b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) The regulations may impose a penalty, not exceeding 50 penalty units, for a contravention of the regulations.

Authorised Version C2025C00651 registered 28/11/2025

Schedule 1—Amendment of other legislation and transitional and saving provisions

Australian Federal Police Act 1979

1 Division 2 of Part II

Repeal the Division.

2 Transitional and saving provision

Despite the repeal of Division 2 of Part II of the *Australian Federal Police Act 1979* by item 1 of this Schedule:

(a) any warrant issued under that Division and in force immediately before the day of that repeal remains in force, according to its terms, after that day as if that Division had not been repealed; and

(b) any consent by a Judge of a court created by the Parliament to be nominated by the Minister under subsection 12D(2) of the *Australian Federal Police Act 1979*, being a consent that is in force immediately before the day of that repeal, is to be treated, with effect from that day, as if it were a consent to be declared by the Minister to be an eligible Judge under subsection 12(3) of the *Surveillance Devices Act 2004*; and

(c) any nomination by the Minister of a Judge of a court created by the Parliament as a Judge who may issue warrants under section 12G of the *Australian Federal Police Act 1979*, being a nomination that was in force immediately before the day of that repeal, is to be treated, with effect from that day, as if it were a nomination of that Judge as an eligible Judge for the purposes of section 12 of the *Surveillance Devices Act 2004*; and

(d) any nomination by the Minister of a person holding an appointment referred to in subsection 12DA(1) of the *Australian Federal Police Act 1979*, being a nomination that was in force immediately before the day of that repeal, is taken, with effect from that day, to be a nomination of that person for the purposes of section 13 of the *Surveillance Devices Act 2004*.

Authorised Version C2025C00651 registered 28/11/2025

3 Operation of Division 2 of Part II of the *Australian Federal Police Act 1979* preserved for limited purposes

Despite the repeal of Division 2 of Part II of the *Australian Federal Police Act 1979* by item 1 of this Schedule, that Division is to be treated as continuing to apply in relation to the use of listening devices in respect of offences against the law of the Australian Capital Territory as if:

(a) the Division had not been repealed; and

(b) the definitions of ***class 1 general offence*** and ***class 2 general offence*** and the definition of ***general offence*** were limited to offences against the law of the Australian Capital Territory; and

(c) for the purposes of the continued operation of section 12L of the *Australian Federal Police Act 1979*:

(i) sections 219F to 219K of the *Customs Act 1901* had not been repealed; and

(ii) references in section 12L of the *Australian Federal Police Act 1979* to general offences, class 1 general offences or class 2 general offences were to be construed as if limited to offences against the law of the Australian Capital Territory.

Customs Act 1901

5 Division 1A of Part XII

Repeal the Division.

6 Transitional and saving provision

Despite the repeal of Division 1A of Part XII of the *Customs Act 1901* by item 5 of this Schedule:

(a) any warrant issued under that Division and in force immediately before the day of that repeal remains in force, according to its terms, after that day as if that Division had not been repealed; and

(b) any consent by a Judge of a court created by the Parliament to be nominated by the Minister under subsection 219AA(1) of the *Customs Act 1901*, being a consent that is in force immediately before the day of that repeal, is to be treated,

Authorised Version C2025C00651 registered 28/11/2025

with effect from that day, as if it were a consent to be declared by the Minister to be an eligible Judge under subsection 12(3) of the *Surveillance Devices Act 2004*; and

(c) any nomination by the Minister of a Judge of a court created by the Parliament as a Judge who may issue warrants under that Division, being a nomination that was in force immediately before the day of that repeal, is to be treated, with effect from that day, as if it were a nomination of that Judge as an eligible Judge for the purposes of section 12 of the *Surveillance Devices Act 2004*; and

(d) any nomination by the Minister of a person holding an appointment referred to in subsection 219AB(1) of the *Customs Act 1901*, being a nomination that was in force immediately before the day of that repeal, is taken, with effect from that day, to be a nomination of that person for the purposes of section 13 of the *Surveillance Devices Act 2004*.

Authorised Version C2025C00651 registered 28/11/2025

Endnotes

Endnote 1—About the endnotes

The endnotes provide information about this compilation and the compiled law.

The following endnotes are included in every compilation:

Endnote 1—About the endnotes
Endnote 2—Abbreviation key
Endnote 3—Legislation history
Endnote 4—Amendment history

Abbreviation key—Endnote 2
The abbreviation key sets out abbreviations that may be used in the endnotes.

Legislation history and amendment history—Endnotes 3 and 4
Amending laws are annotated in the legislation history and amendment history.

The legislation history in endnote 3 provides information about each law that has amended (or will amend) the compiled law. The information includes commencement details for amending laws and details of any application, saving or transitional provisions that are not included in this compilation.

The amendment history in endnote 4 provides information about amendments at the provision (generally section or equivalent) level. It also includes information about any provision of the compiled law that has been repealed in accordance with a provision of the law.

Editorial changes
The *Legislation Act 2003* authorises First Parliamentary Counsel to make editorial and presentational changes to a compiled law in preparing a compilation of the law for registration. The changes must not change the effect of the law. Editorial changes take effect from the compilation registration date.

If the compilation includes editorial changes, the endnotes include a brief outline of the changes in general terms. Full details of any changes can be obtained from the Office of Parliamentary Counsel.

Misdescribed amendments
A misdescribed amendment is an amendment that does not accurately describe how an amendment is to be made. If, despite the misdescription, the amendment

Authorised Version C2025C00651 registered 28/11/2025

can be given effect as intended, then the misdescribed amendment can be incorporated through an editorial change made under section 15V of the *Legislation Act 2003*.

If a misdescribed amendment cannot be given effect as intended, the amendment is not incorporated and "(md not incorp)" is added to the amendment history.

Authorised Version C2025C00651 registered 28/11/2025

Endnote 2—Abbreviation key

ad = added or inserted

am = amended

amdt = amendment

C[x] = Compilation No. x

ch = Chapter(s)

cl = clause(s)

cont. = continued

def = definition(s)

Dict = Dictionary

disallowed = disallowed by Parliament

div = Division(s)

ed = editorial change

exp = expires/expired or ceases/ceased to have effect

gaz = gazette

LA = *Legislation Act 2003*

LIA = *Legislative Instruments Act 2003*

(md) = misdescribed amendment can be given effect

(md not incorp) = misdescribed amendment cannot be given effect

mod = modified/modification

No. = Number(s)

Ord = Ordinance

orig = original

p = page(s)

para = paragraph(s)/subparagraph(s) /sub-subparagraph(s)

pres = present

prev = previous

(prev…) = previously

pt = Part(s)

r = regulation(s)/Court rule(s)

reloc = relocated

renum = renumbered

rep = repealed

rs = repealed and substituted

s = section(s)/subsection(s) /rule(s)/subrule(s)/order(s)/suborder(s)

sch = Schedule(s)

SLI = Select Legislative Instrument

SR = Statutory Rules

sub ch = Sub-Chapter(s)

sub div = Subdivision(s)

sub pt = Subpart(s)

underlining = whole or part not commenced or to be commenced

Authorised Version C2025C00651 registered 28/11/2025

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Surveillance Devices Act 2004	152, 2004	15 Dec 2004	15 Dec 2004 (s 2)	
Law and Justice Legislation Amendment (Serious Drug Offences and Other Measures) Act 2005	129, 2005	8 Nov 2005	Sch 1 (items 68, 69, 75, 76): 6 Dec 2005 (s 2(1) item 2)	Sch 1 (items 75, 76)
Law and Justice Legislation Amendment (Video Link Evidence and Other Measures) Act 2005	136, 2005	15 Nov 2005	16 Nov 2005 (s 2)	—
Anti-Terrorism Act (No. 2) 2005	144, 2005	14 Dec 2005	Sch 7 (items 15–18): 11 Jan 2006 (s 2(1) item 7) Sch 9 (item 24): never commenced (s 2(1) item 19)	
as amended by				
Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Act 2006	170, 2006	12 Dec 2006	Sch 1 (item 11): 14 Dec 2005 (s 2(1) item 3)	—
Statute Law Revision Act 2006	9, 2006	23 Mar 2006	Sch 1 (items 25, 26): 15 Dec 2004 (s 2(1) item 17)	—

Authorised Version C2025C00651 registered 28/11/2025

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications (Interception) Amendment Act 2006	40, 2006	3 May 2006	Sch 1 (items 23, 24): 13 June 2006 (s 2(1) item 2)	—
Law Enforcement Integrity Commissioner (Consequential Amendments) Act 2006	86, 2006	30 June 2006	Sch 1 (items 60–70): 30 Dec 2006 (s 2(1))	—
Anti-Money Laundering and Counter-Terrorism Financing (Transitional Provisions and Consequential Amendments) Act 2006	170, 2006	12 Dec 2006	Sch 1 (item 158): 13 Dec 2006 (s 2(1) item 24)	—
Law and Justice Legislation Amendment (Marking of Plastic Explosives) Act 2007	3, 2007	19 Feb 2007	Sch 3 (item 6): 25 Aug 2007 (s 2(1) item 2)	—
Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2007	52, 2007	12 Apr 2007	Sch 1 (items 63, 64): 13 Apr 2007 (s 2(1) items 7, 8)	—
Fisheries Legislation Amendment Act 2007	104, 2007	28 June 2007	Sch 4: 26 July 2007 (s 2(1) item 5)	—
Telecommunications Interception Legislation Amendment Act 2008	95, 2008	3 Oct 2008	Sch 1: 4 Oct 2008 (s 2(1) item 2)	Sch 1 (items 9, 10)
Telecommunications Interception Legislation Amendment Act (No. 1) 2009	32, 2009	22 May 2009	Sch 2 (item 1): 23 May 2009(s 2(1) item 3)	—

Authorised Version C2025C00651 registered 28/11/2025

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Crimes Legislation Amendment (Serious and Organised Crime) Act (No. 2) 2010	4, 2010	19 Feb 2010	Sch 7 (items 24, 29): 20 Feb 2010 (s 2(1) item 2)	Sch 7 (item 29)
Crimes Legislation Amendment (Sexual Offences Against Children) Act 2010	42, 2010	14 Apr 2010	Sch 1 (items 72–74): 15 Apr 2010 (s 2(1) item 2)	Sch 1 (item 74)
Anti-People Smuggling and Other Measures Act 2010	50, 2010	31 May 2010	Sch 1 (items 14–16): 1 June 2010 (s 2)	Sch 1 (item 16)
Acts Interpretation Amendment Act 2011	46, 2011	27 June 2011	Sch 2 (items 1099–1101) and Sch 3 (items 10, 11): 27 Dec 2011 (s 2(1) items 11, 12)	Sch 3 (items 10, 11)
Extradition and Mutual Assistance in Criminal Matters Legislation Amendment Act 2012	7, 2012	20 Mar 2012	Sch 3 (items 51, 52, 54–69) and Sch 4 (item 4): 20 Sept 2012 (s 2(1) items 8, 10, 14) Sch 3 (item 53): never commenced (s 2(1) item 9)	Sch 3 (item 69)
Crimes Legislation Amendment (Powers and Offences) Act 2012	24, 2012	4 Apr 2012	Sch 4 (item 53): 5 Apr 2012 (s 2(1) item 7)	—
Statute Law Revision Act 2012	136, 2012	22 Sept 2012	Sch 6 (items 76–79): 22 Sept 2012 (s 2(1) item 37)	—
Law Enforcement Integrity Legislation Amendment Act 2012	194, 2012	12 Dec 2012	Sch 1 (items 47–78, 91(1), (2)): 13 Dec 2012 (s 2(1) item 4)	Sch 1 (item 91(1), (2))
Statute Law Revision Act (No. 1) 2014	31, 2014	27 May 2014	Sch 4 (item 54): 24 June 2014 (s 2(1) item 9)	—

Authorised Version C2025C00651 registered 28/11/2025

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
National Security Legislation Amendment Act (No. 1) 2014	108, 2014	2 Oct 2014	Sch 2 (item 54): 30 Oct 2014 (s 2(1) item 2)	—
Statute Law Revision Act (No. 1) 2015	5, 2015	25 Feb 2015	Sch 1 (item 42): 25 Mar 2015 (s 2(1) item 2)	—
Crimes Legislation Amendment (Psychoactive Substances and Other Measures) Act 2015	12, 2015	5 Mar 2015	Sch 6 (item 16): 6 Mar 2015 (s 2(1) item 7)	—
Customs and Other Legislation Amendment (Australian Border Force) Act 2015	41, 2015	20 May 2015	Sch 5 (items 149–151) and Sch 9): 1 July 2015 (s 2(1) items 2, 9)	Sch 5 (item 151) and Sch 9
as amended by				
Australian Border Force Amendment (Protected Information) Act 2017	115, 2017	30 Oct 2017	Sch 1 (item 26): 1 July 2015 (s 2(1) item 2)	—
Tribunals Amalgamation Act 2015	60, 2015	26 May 2015	Sch 8 (item 44) and Sch 9: 1 July 2015 (s 2(1) items 19, 22)	Sch 9
Acts and Instruments (Framework Reform) (Consequential Provisions) Act 2015	126, 2015	10 Sept 2015	Sch 1 (item 595): 5 Mar 2016 (s 2(1) item 2)	—
Statute Law Revision Act (No. 2) 2015	145, 2015	12 Nov 2015	Sch 1 (item 15): 10 Dec 2015 (s 2(1) item 2)	—
Crimes Legislation Amendment (Powers, Offences and Other Measures) Act 2015	153, 2015	26 Nov 2015	Sch 15 (items 14–31): 27 Nov 2015 (s 2(1) item 3)	Sch 1 (item 30)

Authorised Version C2025C00651 registered 28/11/2025

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Counter-Terrorism Legislation Amendment Act (No. 1) 2016	82, 2016	29 Nov 2016	Sch 10: 30 Nov 2016 (s 2(1) item 2)	—
Law Enforcement Legislation Amendment (State Bodies and Other Measures) Act 2016	86, 2016	30 Nov 2016	Sch 1 (items 1, 56–58) and Sch 2 (items 5, 6): 1 Dec 2016 (s 2(1) items 2, 4, 5) Sch 1 (items 37–41, 54, 55): 1 July 2017 (s 2(1) item 3)	Sch 1 (items 1, 39–41, 54–58)
Criminal Code Amendment (High Risk Terrorist Offenders) Act 2016	95, 2016	7 Dec 2016	Sch 2 (item 1): 7 June 2017 (s 2(1) item 3)	—
Home Affairs and Integrity Agencies Legislation Amendment Act 2018	31, 2018	9 May 2018	Sch 2 (items 182–187, 284): 11 May 2018 (s 2(1) items 3, 7)	Sch 2 (item 284)
Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018	34, 2018	22 May 2018	Sch 1 (items 5, 6, 11, 84–100): 22 Nov 2018 (s 2(1) item 2)	Sch 1 (items 11, 100)
Investigation and Prosecution Measures Act 2018	37, 2018	22 May 2018	Sch 1 (items 1, 11–18): 22 May 2018 (s 2(1) item 2)	Sch 1 (items 1, 12–18)
National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018	67, 2018	29 June 2018	Sch 1 (items 49, 50): 30 June 2018 (s 2(1) item 2)	—

Authorised Version C2025C00651 registered 28/11/2025

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018	148, 2018	8 Dec 2018	Sch 2 (items 27–60, 60A, 61–88, 90, 91, 91A, 92–104, 104A, 105–111, 111A, 112, 113, 113A, 113B, 114–119, 132, 135–146): 9 Dec 2018 (s 2(1) items 4, 5)	Sch 2 (items 132, 146)
Combatting Child Sexual Exploitation Legislation Amendment Act 2019	72, 2019	20 Sept 2019	Sch 2 (item 8): 21 Sept 2019 (s 2(1) item 3)	—
Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020	133, 2020	17 Dec 2020	Sch 1 (item 122): 17 June 2022 (s 2(1) item 3)	—
Telecommunications Legislation Amendment (International Production Orders) Act 2021	78, 2021	23 July 2021	Sch 1 (item 46): 24 July 2021 (s 2(1) item 4)	—
Surveillance Legislation Amendment (Identify and Disrupt) Act 2021	98, 2021	3 Sept 2021	Sch 1 (items 1–51), Sch 2 (items 1–32) and Sch 5 (items 1–6): 4 Sept 2021 (s 2(1) items 2–4)	—
Counter-Terrorism Legislation Amendment (High Risk Terrorist Offenders) Act 2021	131, 2021	8 Dec 2021	Sch 1 (items 211–312): 9 Dec 2021 (s 2(1) item 2)	—

Authorised Version C2025C00651 registered 28/11/2025

Endnote 3—Legislation history

Act	Number and year	Assent	Commencement	Application, saving and transitional provisions
National Anti-Corruption Commission (Consequential and Transitional Provisions) Act 2022	89, 2022	12 Dec 2022	sch 1 (items 188-200B), sch 2 (items 1, 30, 31): 1 July 2023 (s 2(1) items 2, 3)	sch 2 (items 1, 30, 31)
Crimes and Other Legislation Amendment (Omnibus) Act 2023	63, 2023	13 Sept 2023	sch 10 (items 7, 8): 14 Sept 2023 (s 2(1) item 8)	—
Inspector-General of Intelligence and Security and Other Legislation Amendment (Modernisation) Act 2023	73, 2023	20 Sept 2023	sch 1 (item 199), sch 3 (item 2): 21 Sept 2023 (s 2(1) items 2, 5)	sch 3 (item 2)

Act (Register ID)	Number and year	Assent	Commencement	Application, saving and transitional provisions
Statute Law Amendment (Prescribed Forms and Other Updates) Act 2023 (C2023A00074)	74, 2023	20 Sept 2023	sch 3 (item 14): 18 Oct 2023 (s 2(1) item 3)	—
Australian Citizenship Amendment (Citizenship Repudiation) Act 2023 (C2023A00109)	109, 2023	7 Dec 2023	sch 1 (item 17): 8 Dec 2023 (s 2(1) item 1)	—

Authorised Version C2025C00651 registered 28/11/2025

Endnote 3—Legislation history

Act (Register ID)	Number and year	Assent	Commencement	Application, saving and transitional provisions
Migration and Other Legislation Amendment (Bridging Visas, Serious Offenders and Other Measures) Act 2023 (C2023A00110)	110, 2023	7 Dec 2023	sch 2 (items 6-82, 132): 8 Dec 2023 (s 2(1) item 1)	sch 2 (item 132)
Administrative Review Tribunal (Consequential and Transitional Provisions No. 2) Act 2024 (C2024A00039)	39, 2024	31 May 2024	sch 2 (items 103-163): 14 Oct 2024 (s 2(1) item 2)	—
Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024 (C2024A00110)	110, 2024	10 Dec 2024	sch 11 (item 35): 7 Jan 2025 (s 2(1) item 13)	—
Telecommunications and Other Legislation Amendment Act 2025 (C2025A00053)	53, 2025	4 Nov 2025	sch 1 (items 1-3, 5): 5 Nov 2025 (s 2(1) item 1)	sch 1 (item 5)
Criminal Code Amendment (State Sponsors of Terrorism) Act 2025 (C2025A00060)	60, 2025	6 Nov 2025	sch 2 (items 12-15), sch 3 (items 68, 69): 8 Nov 2025 (s 2(1) item 2)	—

Authorised Version C2025C00651 registered 28/11/2025

Endnote 4—Amendment history

Provision affected	How affected
Title	am No 148, 2018; No 98, 2021
Part 1	
s 3	am No 9, 2006; No 82, 2016; No 148, 2018; No 98, 2021; No 131, 2021
	ed C49
	am No 110, 2023
s 4	am No 82, 2016; No 148, 2018; No 98, 2021; No 131, 2021; No 110, 2023
s 6	am No 86, 2006; No 170, 2006; No 52, 2007; No 104, 2007; No 95, 2008; No 32, 2009; No 4, 2010; No 7, 2012; No 24, 2012; No 194, 2012; No 12, 2015; No 41, 2015; No 153, 2015; No 82, 2016; No 95, 2016; No 34, 2018; No 148, 2018 (amdt never applied (Sch 2 items 40, 41)); No 133, 2020; No 98, 2021; No 131, 2021; No 89, 2022; No 63, 2023; No 74, 2023; No 110, 2023; No 39, 2024; No 110, 2024; No 60, 2025
s 6A	ad No 95, 2008
	rs No 153, 2015
	am No 82, 2016; No 86, 2016; No 37, 2018; No 89, 2022; No 63, 2023
s 6B	ad No 95, 2008
	am No 89, 2022
s 6C	ad No 82, 2016
	rs No 131, 2021
s 6D	ad No 82, 2016
	rs No 131, 2021
s 6E	ad No 110, 2023
s 6F	ad No 110, 2023
s 7A	ad No 98, 2021

Authorised Version C2025C00651 registered 28/11/2025

Endnote 4—Amendment history

Provision affected	How affected
Part 2	
Division 1	
s 10	am No 148, 2018; No 98, 2021
s 11	rs No 89, 2022
	am No 39, 2024
s 12	am No 126, 2015; No 31, 2018; No 89, 2022
s 13	am No 60, 2015; No 31, 2018; No 89, 2022; No 39, 2024
Division 2	
s 14	am No 7, 2012; No 194, 2012; No 82, 2016; No 34, 2018; No 131, 2021; No 110, 2023; No 39, 2024; No 60, 2025
s 15	am No 31, 2014; No 39, 2024
s 16	am No 7, 2012; No 194, 2012; No 82, 2016; No 34, 2018; No 131, 2021; No 110, 2023; No 39, 2024; No 60, 2025
s 17	am No 7, 2012; No 194, 2012; No 82, 2016; No 34, 2018; No 131, 2021; No 110, 2023; No 39, 2024
s 18	am No 40, 2006
s 19	am No 194, 2012; No 131, 2021; No 110, 2023; No 39, 2024
s 20	am No 7, 2012; No 194, 2012; No 82, 2016; No 131, 2021; No 110, 2023; No 39, 2024
s 21	am No 7, 2012; No 194, 2012; No 82, 2016; No 34, 2018; No 131, 2021; No 110, 2023; No 39, 2024
Division 3	
s 22	am No 136, 2005; No 39, 2024
s 23	am No 31, 2014; No 39, 2024
s 24	am No 39, 2024
s 25	am No 39, 2024
s 27	am No 39, 2024
Division 4	
Division 4	ad No 148, 2018
s 27A	ad No 148, 2018
	am No 148, 2018; No 131, 2021; No 110, 2023; No 39, 2024; No 60, 2025

Authorised Version C2025C00651 registered 28/11/2025

Endnote 4—Amendment history

Provision affected	How affected
s 27B	ad No 148, 2018
	am No 39, 2024
s 27C	ad No 148, 2018
	am No 148, 2018; No 131, 2021; No 110, 2023; No 39, 2024; No 60, 2025
s 27D	ad No 148, 2018
	am No 148, 2018
	ed C45
	am No 131, 2021; No 110, 2023; No 39, 2024
s 27E	ad No 148, 2018
	am No 148, 2018
	ed C45
	am No 131, 2021; No 110, 2023; No 39, 2024
s 27F	ad No 148, 2018
	am No 131, 2021; No 110, 2023; No 39, 2024
s 27G	ad No 148, 2018
	am No 131, 2021; No 110, 2023; No 39, 2024
s 27H	ad No 148, 2018
	am No 148, 2018; No 131, 2021; No 110, 2023; No 39, 2024
s 27J	ad No 148, 2018
Division 5	
Division 5	ad No 98, 2021
	exp 3 Sept 2026 (s 27KAA)
s 27KAA	ad No 98, 2021
	exp 3 Sept 2026 (s 27KAA)
s 27KA	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KAA)
s 27KB	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KAA)

Authorised Version C2025C00651 registered 28/11/2025

Provision affected	How affected
s 27KBA	ad No 98, 2021
	exp 3 Sept 2026 (s 27KAA)
s 27KBB	ad No 98, 2021
	exp 3 Sept 2026 (s 27KAA)
s 27KC	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KAA)
s 27KD	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KAA)
s 27KE	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KAA)
s 27KF	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KAA)
s 27KG	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KAA)
s 27KH	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KAA)
s 27KJ	ad No 98, 2021
	exp 3 Sept 2026 (s 27KAA)
Division 6	
Division 6	ad No 98, 2021
	exp 3 Sept 2026 (s 27KKA)
s 27KKA	ad No 98, 2021
	exp 3 Sept 2026 (s 27KKA)
s 27KK	ad No 98, 2021
	am No 39, 2024

Endnote 4—Amendment history

Provision affected	How affected
	exp 3 Sept 2026 (s 27KKA)
s 27KL	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KKA)
s 27KM	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KKA)
s 27KN	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KKA)
s 27KP	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KKA)
s 27KQ	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KKA)
s 27KR	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KKA)
s 27KS	ad No 98, 2021
	am No 39, 2024
	exp 3 Sept 2026 (s 27KKA)
s 27KT	ad No 98, 2021
	exp 3 Sept 2026 (s 27KKA)
Part 3	
s 27KU	ad No 98, 2021
s 28	am No 31, 2014; No 148, 2018; No 98, 2021
	(1C), (1D) exp 3 Sept 2026 (s 27KU(1))
s 29	am No 31, 2014; No 148, 2018

Authorised Version C2025C00651 registered 28/11/2025

Provision affected	How affected
s 30	am No 129, 2005; No 144, 2005; No 3, 2007; No 42, 2010; No 50, 2010; No 31, 2014; No 5, 2015; No 67, 2018; No 148, 2018; No 72, 2019; No 60, 2025
s 31	am No 126, 2015
s 32	am No 40, 2006; No 148, 2018; No 98, 2021
s 33	am No 126, 2015; No 148, 2018; No 98, 2021; No 89, 2022; No 39, 2024
s 34	am No 148, 2018; No 98, 2021; No 39, 2024
s 35	am No 148, 2018; No 39, 2024
s 35A	ad No 148, 2018
	am No 39, 2024
s 35B	ad No 98, 2021
	am No 39, 2024
s 36	am No 148, 2018; No 98, 2021
s 36A	ad No 98, 2021
Part 4	
s 37	am No 9, 2006; No 86, 2006; No 82, 2016; No 131, 2021; No 89, 2022; No 110, 2023
s 38	am No 86, 2006; No 82, 2016
	ed C47
	am No 131, 2021; No 89, 2022; No 110, 2023
s 39	am No 136, 2005; No 194, 2012; No 82, 2016; No 131, 2021; No 110, 2023
s 40	am No 194, 2012; No 126, 2015; No 82, 2016; No 131, 2021; No 110, 2023
Part 5	
s 41	am No 46, 2011; No 148, 2018; No 98, 2021
s 42	am No 104, 2007; No 126, 2015; No 31, 2018; No 148, 2018; No 78, 2021; No 39, 2024
s 43A	ad No 148, 2018
	am No 98, 2021; No 39, 2024
s 43B	ad No 148, 2018

Authorised Version C2025C00651 registered 28/11/2025

Endnote 4—Amendment history

Provision affected	How affected
s 43C	ad No 98, 2021
	am No 39, 2024
s 43D	ad No 98, 2021
s 43E	ad No 98, 2021
	am No 39, 2024
Part 6	
Division 1	
s 44	am No 46, 2011; No 148, 2018; No 98, 2021; No 39, 2024
s 44A	ad No 98, 2021
s 45	am No 7, 2012; No 194, 2012; No 108, 2014; No 145, 2015; No 153, 2015; No 82, 2016; No 34, 2018; No 98, 2021; No 131, 2021; No 73, 2023; No 109, 2023; No 110, 2023
s 45A	ad No 194, 2012
	am No 89, 2022
s 45B	ad No 98, 2021
	am No 53, 2025
s 46	am No 194, 2012; No 148, 2018; No 98, 2021
s 46AA	ad No 98, 2021
s 46A	ad No 82, 2016
	am No 148, 2018; No 131, 2021
s 46B	ad No 110, 2023
s 47A	ad No 148, 2018
	am No 98, 2021
s 47B	ad No 98, 2021
Division 2	
s 49	am No 194, 2012; No 82, 2016; No 148, 2018; No 98, 2021; No 131, 2021
	ed C49
	am No 110, 2023
s 49A	ad No 82, 2016
	am No 148, 2018

Authorised Version C2025C00651 registered 28/11/2025

Provision affected	How affected
	rs No 131, 2021
	am No 110, 2023
s 49B	ad No 148, 2018
s 49C	ad No 98, 2021
s 49D	ad No 98, 2021
s 50	am No 7, 2012; No 82, 2016; No 34, 2018; No 148, 2018; No 98, 2021
s 50A	ad No 82, 2016
	am No 148, 2018; No 131, 2021; No 110, 2023
s 51	am No 82, 2016; No 148, 2018; No 98, 2021
s 52	am No 126, 2015; No 82, 2016; No 148, 2018; No 98, 2021; No 110, 2023
s 53	am No 7, 2012; No 194, 2012; No 126, 2015; No 82, 2016; No 34, 2018; No 148, 2018; No 131, 2021; No 110, 2023; No 39, 2024
Division 3	
s 55	am No 82, 2016; No 148, 2018; No 98, 2021; No 131, 2021; No 110, 2023
s 61	am No 82, 2016; No 131, 2021; No 110, 2023
s 61A	ad No 82, 2016
	am No 131, 2021; No 110, 2023
Division 4	
s 62	am No 148, 2018; No 98, 2021
Part 7	
s 64	am No 86, 2006; No 148, 2018; No 98, 2021; No 89, 2022
s 64A	ad No 148, 2018
	am No 148, 2018
	ed C45
	am No 98, 2021; No 131, 2021; No 89, 2022; No 110, 2023; No 39, 2024
s 64B	ad No 98, 2021
	am No 39, 2024
s 65	am No 148, 2018; No 98, 2021

Authorised Version C2025C00651 registered 28/11/2025

Endnote 4—Amendment history

Provision affected	How affected
s 65A	ad No 82, 2016
	am No 148, 2018; No 131, 2021
s 65B	ad No 82, 2016
	am No 148, 2018; No 131, 2021
s 65C	ad No 98, 2021
Schedule 1	
Schedule 1	am No 136, 2012

Authorised Version C2025C00651 registered 28/11/2025