



# Telecommunications (Interception and Access) Regulations 2017

made under the

*Telecommunications (Interception and Access) Act 1979*

## Compilation No. 4

**Compilation date:** 3 December 2019

**Includes amendments up to:** F2019L01552

**Registered:** 11 December 2019

Prepared by the Office of Parliamentary Counsel, Canberra

---

## About this compilation

### This compilation

This is a compilation of the *Telecommunications (Interception and Access) Regulations 2017* that shows the text of the law as amended and in force on 3 December 2019 (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. Any uncommenced amendments affecting the law are accessible on the Legislation Register ([www.legislation.gov.au](http://www.legislation.gov.au)). The details of amendments made up to, but not commenced at, the compilation date are underlined in the endnotes. For more information on any uncommenced amendments, see the series page on the Legislation Register for the compiled law.

### Application, saving and transitional provisions for provisions and amendments

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.

### 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. For more information on any modifications, see the series page on the Legislation Register for the compiled law.

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If a provision of the compiled law has been repealed in accordance with a provision of the law, details are included in the endnotes.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

<b>Part 1—Preliminary</b>	1
1 Name	1
3 Authority	1
5 Definitions	1
<b>Part 2—General matters</b>	2
6 Criminal organisation—prescribed provision	2
7 Proceeding for confiscation or forfeiture or for pecuniary penalty—prescribed Acts	2
8 Warrants authorising agencies to intercept telecommunications—prescribed forms	2
9 Stored communications warrant—prescribed form	3
10 Journalist information warrant—prescribed form	3
<b>Part 3—Access to telecommunications data</b>	4
<b>Division 1—Journalist information warrants</b>	4
11 Public Interest Advocate to be given proposed journalist information warrant requests made by the Director-General of Security	4
12 Public Interest Advocate to be given proposed journalist information warrant applications made by an enforcement agency	4
13 Public Interest Advocate to deal with proposed journalist information warrant requests and applications	5
14 Public Interest Advocate to prepare submissions	6
15 Public Interest Advocate’s attendance at hearing of oral application by an enforcement agency for a proposed journalist information warrant	7
16 Further information, or a copy or summary of information, to be given to Public Interest Advocate	8
17 Public Interest Advocate to return proposed journalist information warrant requests and applications	9
<b>Division 2—Public Interest Advocates</b>	11
18 Eligibility for appointment	11
19 Term of appointment	11
20 Remuneration	11
21 Disclosure of interests	12
22 Conflicts of interest	12
23 Resignation	12
24 Termination of appointment	13
25 Immunity from legal action	13
<b>Division 3—Miscellaneous</b>	14
26 Arrangements with States and Territories	14
<b>Part 4—Transitional matters</b>	15
27 Things done under the <i>Telecommunications (Interception and Access) Regulations 1987</i>	15

---

<b>Schedule 1—Forms of warrants</b>	16
<b>Form 1—Telecommunications service warrant</b>	16
<b>Form 2—Telecommunications service warrant—B-party</b>	18
<b>Form 2A—Telecommunications service control order warrant</b>	20
<b>Form 2B—Telecommunications service control order warrant—B-party</b>	24
<b>Form 3—Named person warrant—telecommunications services</b>	28
<b>Form 4—Named person warrant—telecommunications devices</b>	31
<b>Form 4A—Named person control order warrant— telecommunications services</b>	34
<b>Form 4B—Named person control order warrant— telecommunications devices</b>	38
<b>Form 5—Warrant for entry on premises and interception of communications</b>	42
<b>Form 5A—Control order warrant for entry on premises and interception of communications</b>	45
<b>Form 6—Stored communications warrant—domestic</b>	48
<b>Form 6A—Stored communications warrant—international</b>	51
<b>Form 7—Journalist information warrant</b>	54
<b>Endnotes</b>	56
<b>Endnote 1—About the endnotes</b>	56
<b>Endnote 2—Abbreviation key</b>	57
<b>Endnote 3—Legislation history</b>	58
<b>Endnote 4—Amendment history</b>	59

## **Part 1—Preliminary**

### **1 Name**

This instrument is the *Telecommunications (Interception and Access) Regulations 2017*.

### **3 Authority**

This instrument is made under the *Telecommunications (Interception and Access) Act 1979*.

### **5 Definitions**

In this instrument:

*Act* means the *Telecommunications (Interception and Access) Act 1979*.

## Part 2—General matters

### 6 Criminal organisation—prescribed provision

For the purposes of paragraph (b) of the definition of *criminal organisation* in subsection 5(1) of the Act, section 7 of the *Serious Crime Control Act 2009* (NT) is prescribed.

Note: Section 7 of the *Serious Crime Control Act 2009* (NT) describes an organisation declared under section 15 of that Act.

### 7 Proceeding for confiscation or forfeiture or for pecuniary penalty—prescribed Acts

For the purposes of paragraph 6K(c) of the Act, each of the following is prescribed:

- (a) the *Proceeds of Crime Act 2002*;
- (b) the *Confiscation of Proceeds of Crime Act 1989* (NSW);
- (c) the *Criminal Assets Recovery Act 1990* (NSW);
- (d) the *Confiscation Act 1997* (Vic);
- (e) the *Criminal Proceeds Confiscation Act 2002* (Qld);
- (f) the *Criminal Property Confiscation Act 2000* (WA);
- (g) the *Criminal Assets Confiscation Act 2005* (SA);
- (h) the *Crime (Confiscation of Profits) Act 1993* (Tas);
- (i) the *Confiscation of Criminal Assets Act 2003* (ACT);
- (j) the *Criminal Property Forfeiture Act 2002* (NT).

### 8 Warrants authorising agencies to intercept telecommunications—prescribed forms

For the purposes of subsection 49(1) of the Act, the following forms are prescribed:

- (a) for a warrant issued under subsection 46(1) of the Act to which subparagraph 46(1)(d)(i) of the Act applies—Form 1 in Schedule 1;
- (b) for a warrant issued under subsection 46(1) of the Act to which subparagraph 46(1)(d)(ii) of the Act applies—Form 2 in Schedule 1;
- (ba) for a control order warrant issued under subsection 46(4) of the Act to which subparagraph 46(4)(d)(i) of the Act applies—Form 2A in Schedule 1;
- (bb) for a control order warrant issued under subsection 46(4) of the Act to which subparagraph 46(4)(d)(ii) of the Act applies—Form 2B in Schedule 1;
- (c) for a warrant issued under subsection 46A(1) of the Act to which subparagraph 46A(1)(d)(i) of the Act applies—Form 3 in Schedule 1;
- (d) for a warrant issued under subsection 46A(1) of the Act to which subparagraph 46A(1)(d)(ii) of the Act applies—Form 4 in Schedule 1;

## Section 9

- 
- (e) for a control order warrant issued under subsection 46A(2A) of the Act to which subparagraph 46A(2A)(e)(i) of the Act applies—Form 4A in Schedule 1;
  - (f) for a control order warrant issued under subsection 46A(2A) of the Act to which subparagraph 46A(2A)(e)(ii) of the Act applies—Form 4B in Schedule 1;
  - (g) for a warrant issued under section 48 of the Act in circumstances mentioned in subsection 46(1) of the Act—Form 5 in Schedule 1;
  - (h) for a control order warrant issued under section 48 of the Act in circumstances mentioned in subsection 46(4) of the Act—Form 5A in Schedule 1.

**9 Stored communications warrant—prescribed form**

For the purposes of paragraph 118(1)(a) of the Act, the following forms are prescribed:

- (a) for a stored communications warrant issued as a result of an application other than an international assistance application—Form 6 in Schedule 1;
- (b) for a stored communications warrant issued as a result of an international assistance application—Form 6A in Schedule 1.

**10 Journalist information warrant—prescribed form**

For the purposes of subsection 180U(1) of the Act, Form 7 in Schedule 1 is prescribed.

## Part 3—Access to telecommunications data

### Division 1—Journalist information warrants

#### 11 Public Interest Advocate to be given proposed journalist information warrant requests made by the Director-General of Security

- (1) Before requesting a journalist information warrant under section 180J of the Act, the Director-General of Security must ensure that a copy of the proposed request is given to a Public Interest Advocate who:
  - (a) has been cleared for security purposes to the same level, and at the same frequency, as that required of an ASIO employee; or
  - (b) satisfies paragraph 18(1)(b) of this instrument.
- (2) If:
  - (a) a copy of a proposed request is given to a Public Interest Advocate, as required by subsection (1); and
  - (b) subparagraph 13(1)(b)(ii) applies;the Director-General of Security must ensure that a copy of the proposed request is given to another Public Interest Advocate in accordance with this section.

#### 12 Public Interest Advocate to be given proposed journalist information warrant applications made by an enforcement agency

- (1) Before making a written application for a journalist information warrant under section 180Q of the Act, the person making the application on behalf of an enforcement agency must ensure that a Public Interest Advocate is given a copy of the proposed application.
- (2) Before making an oral application for a journalist information warrant under section 180Q of the Act, the person making the application on behalf of an enforcement agency must ensure that a Public Interest Advocate is notified of the proposed application.
- (3) If:
  - (a) both:
    - (i) a copy of a proposed application is given to a Public Interest Advocate, as required by subsection (1); and
    - (ii) subparagraph 13(1)(b)(ii) applies; or
  - (b) both:
    - (i) a Public Interest Advocate is notified of a proposed application, as required by subsection (2); and
    - (ii) the Public Interest Advocate advises that he or she is unable to attend the hearing of the application;the person making the application must ensure that a copy of the proposed application is given to another Public Interest Advocate in accordance with this section.



---

### **13 Public Interest Advocate to deal with proposed journalist information warrant requests and applications**

#### *Requests and written applications*

- (1) Upon receiving a proposed request by the Director-General of Security or written application by an enforcement agency for a journalist information warrant, the relevant Public Interest Advocate:
  - (a) may consider the proposed request or application; and
  - (b) must, as soon as reasonably practicable, advise the applicant that:
    - (i) he or she will prepare a submission in relation to the proposed request or application; or
    - (ii) he or she is unable to prepare a submission in relation to the proposed request or application.

#### *Oral applications*

- (2) Upon being notified about a proposed oral application by an enforcement agency for a journalist information warrant, the relevant Public Interest Advocate must advise the applicant whether he or she is able to attend the hearing of the application.

Note: See section 15.

#### *Further information relating to requests or applications*

- (3) If:
  - (a) further information is given to:
    - (i) the Attorney-General in relation to a request by the Director-General of Security; or
    - (ii) the relevant Part 4-1 issuing authority in relation to an application by an enforcement agency; and
  - (b) a Public Interest Advocate is also given the further information or a summary of it;then:
  - (c) in the case of a request by the Director-General of Security for a journalist information warrant, subsection (1) applies as if the further information or summary were a proposed request for such a warrant; and
  - (d) in the case of a written application by an enforcement agency for a journalist information warrant, subsection (1) applies as if the further information or summary were a proposed written application for such a warrant; and
  - (e) in the case of an oral application by an enforcement agency for a journalist information warrant, subsection (2) applies as if the further information or summary were a proposed oral application for such a warrant.

## Section 14

---

### **14 Public Interest Advocate to prepare submissions**

#### *Submission to be prepared*

- (1) If subparagraph 13(1)(b)(i) applies, the relevant Public Interest Advocate must prepare a submission relating to the proposed request by the Director-General of Security or application by an enforcement agency, and endeavour to do so within a reasonable period, but no later than 7 days after being given the proposed request or application.
- (2) The Public Interest Advocate must include in the submission the facts and considerations he or she considers:
  - (a) are relevant to one or both of the following:
    - (i) the decision whether to issue a journalist information warrant (including any facts and considerations which support the conclusion that a journalist information warrant should not be issued);
    - (ii) the decision about the conditions or restrictions (if any) that are to be specified in the warrant; and
  - (b) have not been satisfactorily addressed in the proposed request by the Director-General of Security or application by the enforcement agency.
- (3) Subsection (2) does not limit the facts or considerations that the Public Interest Advocate may include in his or her submission.
- (4) In determining what is a reasonable period to prepare the submission, the Public Interest Advocate must take into account:
  - (a) the time that could reasonably be expected to be required to prepare the submission; and
  - (b) the gravity of the matter in relation to which the proposed request or application relates; and
  - (c) the urgency of the circumstances in which the proposed request or application is made; and
  - (d) any other matter that the Public Interest Advocate considers relevant.

#### *Copy of submission to be given to relevant person*

- (5) The Public Interest Advocate must, as soon as reasonably practicable, provide a copy of the submission to:
  - (a) in the case of a proposed request by the Director-General of Security—the Director-General of Security; and
  - (b) in the case of a proposed application by an enforcement agency—the following:
    - (i) if the Public Interest Advocate knows the identity of the person who proposes to make the application on behalf of the enforcement agency and that person is available—that person;
    - (ii) in any other case—the chief officer of the enforcement agency that is proposing to make the application.

---

*Submission to take into account further information*

- (6) If:
- (a) further information is given to:
    - (i) the Attorney-General in relation to a request by the Director-General of Security; or
    - (ii) the relevant Part 4-1 issuing authority in relation to an application by an enforcement agency; and
  - (b) a Public Interest Advocate is also given the further information or a summary of it; and
  - (c) subparagraph 13(1)(b)(i) applies;
- the Public Interest Advocate must update the submission, or prepare a new submission, relating to the request or application taking into account the further information or summary.
- (7) The Public Interest Advocate must endeavour to update the submission, or prepare the new submission, within a reasonable period, but no later than 7 days after being given the further information or summary.
- (8) Subsections (2) to (5) apply in relation to updating the submission or preparing the new submission.

*Late submissions*

- (9) If a Public Interest Advocate provides a copy of the submission, or updated submission, after the end of the 7 day period mentioned in subsection (1) or (7), the Attorney-General or Part 4-1 issuing authority may consider the late submission or updated submission.

**15 Public Interest Advocate's attendance at hearing of oral application by an enforcement agency for a proposed journalist information warrant**

- (1) A Public Interest Advocate may attend the hearing of an oral application by an enforcement agency for a journalist information warrant in person, or by telephone or other means of voice communication.
- (2) A Public Interest Advocate attending such a hearing may make submissions to the Part 4-1 issuing authority hearing the application in the presence of the relevant enforcement agency.
- (3) Submissions made by the Public Interest Advocate must include the facts and considerations he or she considers:
- (a) are relevant to one or both of the following:
    - (i) the decision whether to issue a journalist information warrant (including any facts and considerations which support the conclusion that a journalist information warrant should not be issued);
    - (ii) the decision about the conditions or restrictions (if any) that are to be specified in the warrant; and
  - (b) have not been satisfactorily addressed in the enforcement agency's application.

## Section 16

---

- (4) Subsection (3) does not limit the facts or considerations that the Public Interest Advocate may include in his or her submissions.
- (5) If:
  - (a) further information is given to a relevant Part 4-1 issuing authority in relation to an oral application; and
  - (b) a Public Interest Advocate is also given the further information or a summary of it; and
  - (c) the Public Interest Advocate has confirmed his or her availability to attend the hearing of the application;the Public Interest Advocate must update the submission made, or make a new submission, to the Part 4-1 issuing authority taking into account the further information or summary.

### **16 Further information, or a copy or summary of information, to be given to Public Interest Advocate**

#### *Further information relating to a request by the Director-General of Security*

- (1) If, under section 180K of the Act, the Attorney-General requires the Director-General of Security to give to the Attorney-General further information in connection with a request made by the Director-General of Security, the Attorney-General may require that:
  - (a) in the case of further information given in writing—the further information, or a copy of it, be given to a Public Interest Advocate; and
  - (b) in the case of further information given orally—both:
    - (i) the further information, or a summary of it, be given to a Public Interest Advocate; and
    - (ii) the further information or summary be given to the Public Interest Advocate in a particular form, which may be the same form as that in which the further information was given to the Attorney-General or another form.
- (2) In deciding whether to act under subsection (1), the Attorney-General may have regard to the following matters:
  - (a) the extent to which further information would be likely to be relevant to a Public Interest Advocate's preparation of a new submission, or the updating of his or her submission, relating to the request;
  - (b) the gravity of the matter in relation to which the request relates;
  - (c) the urgency of the circumstances in which the request is being made;
  - (d) any other matter that the Attorney-General considers relevant.

#### *Further information relating to an application by an enforcement agency*

- (3) If, under section 180R of the Act, a Part 4-1 issuing authority requires a person to give to the Part 4-1 issuing authority further information in connection with an application by an enforcement agency, the Part 4-1 issuing authority may require that:

Section 17

---

- (a) in the case of further information given in writing—the further information, or a copy of it, be given to a Public Interest Advocate; and
  - (b) in the case of further information given orally—both:
    - (i) the further information, or a summary of it, be given to a Public Interest Advocate; and
    - (ii) the further information or summary be given to the Public Interest Advocate in a particular form, which may be the same form as that in which the further information was given to the Part 4-1 issuing authority or another form.
- (4) In deciding whether to act under subsection (3), a Part 4-1 issuing authority may have regard to the following matters:
- (a) the extent to which further information would be likely to be relevant to a Public Interest Advocate's preparation of a new submission, or the updating of his or her submission, relating to the application;
  - (b) the gravity of the matter in relation to which the application relates;
  - (c) the urgency of the circumstances in which the application is being made;
  - (d) any other matter that the Part 4-1 issuing authority considers relevant.

**17 Public Interest Advocate to return proposed journalist information warrant requests and applications**

- (1) After a decision has been made to issue, or refuse to issue, a journalist information warrant, or a request or application for such a warrant is withdrawn, a Public Interest Advocate must:
- (a) in the case of a request by the Director-General of Security—return the following to the Director-General of Security:
    - (i) the proposed request to which the warrant relates;
    - (ii) any submission prepared by a Public Interest Advocate;
    - (iii) any other document, or a copy of or extract from a document, relating to the proposed request; and
  - (b) in the case of an application by an enforcement agency—return the following to the enforcement agency:
    - (i) the proposed application to which the warrant relates;
    - (ii) any submission prepared by a Public Interest Advocate;
    - (iii) any other document, or a copy of or extract from a document, relating to the proposed application.
- (2) If:
- (a) further information is given to:
    - (i) the Attorney-General in relation to a request by the Director-General of Security; or
    - (ii) the relevant Part 4-1 issuing authority in relation to an application by an enforcement agency; and
  - (b) a Public Interest Advocate is also given the further information or a summary of it;

**Section 17**

---

the Public Interest Advocate must return the document containing the information or summary to the relevant person mentioned in subsection (1).

---

## Division 2—Public Interest Advocates

### 18 Eligibility for appointment

- (1) Before declaring a person to be a Public Interest Advocate, the Prime Minister must be satisfied that:
  - (a) the person is a Queen's Counsel or Senior Counsel who has been cleared for security purposes to a level that the Prime Minister considers appropriate; or
  - (b) the person has served as a judge of:
    - (i) the High Court; or
    - (ii) a court that is or was created by the Parliament under Chapter III of the Constitution; or
    - (iii) the Supreme Court of a State or Territory; or
    - (iv) the District Court (or equivalent) of a State or Territory; but no longer holds a commission as a judge of a court listed in this paragraph.
- (2) However, the following persons may not be declared as a Public Interest Advocate:
  - (a) the Director-General of Security or a Deputy Director-General of Security;
  - (b) an examiner;
  - (c) the Director of Public Prosecutions or a person performing a similar function appointed under the law of a State or Territory;
  - (d) the Solicitor-General of the Commonwealth, or of a State or Territory;
  - (e) a person who is employed by the Commonwealth, a State or Territory;
  - (f) a member of the Parliament of the Commonwealth or a State or the Legislative Assembly of a Territory.

### 19 Term of appointment

A Public Interest Advocate holds office for the period specified in the written instrument declaring the person to be a Public Interest Advocate. The period must not exceed 5 years.

Note: A Public Interest Advocate may be reappointed: see section 33AA of the *Acts Interpretation Act 1901*.

### 20 Remuneration

#### *Entitlement to charge*

- (1) A Public Interest Advocate may charge remuneration for the time spent by the Public Interest Advocate in the performance of his or her role as a Public Interest Advocate.
- (2) Such remuneration is to be borne:

## Section 21

---

- (a) in respect of a request for a journalist information warrant by the Director-General of Security—by the Organisation; and
- (b) in respect of an application for a journalist information warrant by an enforcement agency—by the enforcement agency.

### *Rate of remuneration*

- (3) A Public Interest Advocate may charge for remuneration:
  - (a) per day—at the daily rate payable to senior counsel without the approval of the Attorney-General, as set out in Appendix D of the *Legal Services Directions 2017*; and
  - (b) per hour—at one-sixth of the maximum daily rate mentioned in paragraph (a), up to a maximum of 6 hours per day.

## **21 Disclosure of interests**

A Public Interest Advocate must give written notice to the Prime Minister of all interests, pecuniary or otherwise, that the Public Interest Advocate has or acquires and that conflicts or could conflict with the proper performance of his or her functions.

## **22 Conflicts of interest**

- (1) A Public Interest Advocate must take reasonable steps to avoid any conflict of interest (real or apparent) in connection with the proper performance of his or her functions as a Public Interest Advocate.
- (2) If the Public Interest Advocate believes that he or she has a conflict of interest (real or apparent) in relation to the subject-matter of a proposed request by the Director-General of Security or proposed application by an enforcement agency for a journalist information warrant, the Public Interest Advocate must:
  - (a) in the case of a proposed request by the Director-General of Security—advise the Director-General of Security that he or she is unable to prepare a submission in relation to the proposed request; or
  - (b) in the case of a proposed written application by an enforcement agency—advise the applicant that he or she is unable to prepare a submission in relation to the proposed application; or
  - (c) in the case of a proposed oral application by an enforcement agency—advise the applicant that he or she is unable to attend the hearing of the application.
- (3) To avoid doubt, subsection (2) does not limit subparagraph 13(1)(b)(ii) or subsection 13(2).

## **23 Resignation**

- (1) A Public Interest Advocate may resign from his or her position by giving the Prime Minister a written resignation.



- 
- (2) The resignation takes effect on the day it is received by the Prime Minister or, if a later day is specified in the resignation, on that later day.

## **24 Termination of appointment**

- (1) The Prime Minister may revoke the declaration of a Public Interest Advocate:
- (a) for misbehaviour by the Public Interest Advocate; or
  - (b) if the Public Interest Advocate is unable to perform his or her duties because of physical or mental incapacity.
- (2) The Prime Minister must revoke the declaration of a Public Interest Advocate if:
- (a) the Public Interest Advocate:
    - (i) becomes bankrupt; or
    - (ii) takes steps to take the benefit of any law for the relief of bankrupt or insolvent debtors; or
    - (iii) compounds with one or more of his or her creditors; or
    - (iv) makes an assignment of his or her remuneration for the benefit of one or more of his or her creditors; or
  - (b) the Public Interest Advocate fails, without reasonable excuse, to comply with section 21 or 22; or
  - (c) the Public Interest Advocate is a person mentioned in paragraph 18(1)(a) and either:
    - (i) ceases to be a Queen's Counsel or Senior Counsel; or
    - (ii) ceases to hold a security clearance to a level that the Prime Minister considers appropriate; or
  - (d) the Public Interest Advocate holds a position mentioned in subsection 18(2).

## **25 Immunity from legal action**

No action, suit or proceeding may be brought against a person who is, or has been, a Public Interest Advocate in relation to anything done, or omitted to be done, in good faith by the Public Interest Advocate:

- (a) in the performance, or purported performance, of his or her functions; or
- (b) in the exercise, or purported exercise, of his or her powers.

## **Division 3—Miscellaneous**

### **26 Arrangements with States and Territories**

*Governor-General may make arrangements*

- (1) The Governor-General may make arrangements with:
- (a) the Governor of a State (other than the Northern Territory); and
  - (b) the Chief Minister for the Australian Capital Territory; and
  - (c) the Administrator of the Northern Territory;
- with respect to the administration of provisions of the Act and this instrument relating to journalist information warrants.

*Lack of arrangement does not affect validity of exercise of power or performance of function*

- (2) The validity of the performance of a function, or the exercise of a power, is not affected by the absence of an arrangement under this section covering the performance of the function, or exercise of the power, relating to the provisions mentioned in subsection (1).

## **Part 4—Transitional matters**

### **27 Things done under the *Telecommunications (Interception and Access) Regulations 1987***

- (1) If:
  - (a) a thing was done for a particular purpose under the *Telecommunications (Interception and Access) Regulations 1987* as in force immediately before those Regulations were repealed; and
  - (b) the thing could be done for that purpose under this instrument;the thing has effect for the purposes of this instrument as if it had been done under this instrument.
- (2) Without limiting subsection (1), a reference in that subsection to a thing being done includes a reference to a notice, application or other instrument being given or made.

---

## Schedule 1—Forms of warrants

Note: See sections 8, 9 and 10.

### Form 1—Telecommunications service warrant

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

TELECOMMUNICATIONS SERVICE WARRANT

<i>Telecommunications service</i>	[unique number assigned to the service; any other known unique identifying factors]
<i>Particular *person/*persons</i>	[full known *name/*names, other known names, other known identifying information (e.g. date of birth)]
<i>Applicant agency</i>	[name]

#### 1 Authorisation

- (1) I, [name], \*an eligible Judge/\*a nominated AAT member within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 46 of the Act, authorise interceptions of communications made to or from the telecommunications service mentioned above.
- (2) I am satisfied, on the basis of the information given to me by the applicant agency, that:
  - (a) Division 3 of Part 2-5 of the Act has been complied with in relation to the application for this warrant; and
  - \* (b) because of urgent circumstances, it was necessary to make the application by telephone; and
  - (c) there are reasonable grounds for suspecting that the particular \*person/\*persons mentioned above \*is/\*are using, or \*is/\*are likely to use, the service; and
  - (d) information that would be likely to be obtained by intercepting, under a warrant, communications made to or from the service would be likely to assist in connection with the investigation by the applicant agency of the following \*serious offence/\*serious offences, in which the \*particular person is/\*particular persons are involved:  
[short particulars of the serious offence or serious offences]; and
  - (e) the warrant should be issued having regard to the following matters only:
    - (i) how much the privacy of any person or persons would be likely to be interfered with by intercepting, under a warrant, communications made to or from the service;
    - (ii) the gravity of the conduct constituting the \*offence/\*offences being investigated;
    - (iii) how much the information mentioned in paragraph (d) would be likely to assist in connection with the investigation by the applicant agency of the \*offence/\*offences;

- 
- (iv) to what extent methods of investigating the \*offence/\*offences that do not involve so intercepting communications have been used by, or are available to, the applicant agency;
  - (v) how much the use of such methods would be likely to assist in connection with the investigation by the applicant agency of the \*offence/\*offences;
  - (vi) how much the use of such methods would be likely to prejudice the investigation by the applicant agency of the \*offence/\*offences, whether because of delay or for any other reason;
  - \*(vii) *[if the applicant agency is an interception agency of Victoria]* any submissions made by the Victorian PIM under section 44A of the Act to me;
  - \*(viii) *[if the applicant agency is an interception agency of Queensland]* any submissions made by the Queensland PIM under section 45 of the Act to me.

## 2 Persons who may exercise this authority

Under subsection 55(1) of the Act, the authority conferred by this warrant may be exercised by an officer or staff member of the applicant agency, or another agency, in relation to whom an approval under subsection 55(3) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

## 3 Period for which warrant is in force

- (1) Under section 54 of the Act, this warrant comes into force when it is issued.
- (2) This warrant is in force until *[a date that is not more than 90 days away]*.

## \*4 Conditions

Interceptions under this warrant are subject to the following conditions:  
*[details of conditions]*.

## \*5 Restrictions

Interceptions under this warrant are subject to the following restrictions:  
*[details of restrictions]*.

Dated

.....  
\*Judge/\*nominated AAT member

\* Omit if not applicable

---

## Form 2—Telecommunications service warrant—B-party

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

TELECOMMUNICATIONS SERVICE WARRANT—B-PARTY

<i>Telecommunications service</i>	[unique number assigned to the service; any other known unique identifying factors]
<i>Particular *person/*persons</i>	[full known *name/*names, other known names, other known identifying information (e.g. date of birth)]
<i>Applicant agency</i>	[name]

### 1 Authorisation

- (1) I, [name], \*an eligible Judge/\*a nominated AAT member within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 46 of the Act, authorise interceptions of communications made to or from the telecommunications service mentioned above.
- (2) I am satisfied, on the basis of the information given to me by the applicant agency, that:
  - (a) Division 3 of Part 2-5 of the Act has been complied with in relation to the application for this warrant; and
  - \* (b) because of urgent circumstances, it was necessary to make the application by telephone; and
  - (c) there are reasonable grounds for suspecting that the particular \*person/\*persons mentioned above \*is/\*are using, or \*is/\*are likely to use, the service; and
  - (d) information that would be likely to be obtained by intercepting, under a warrant, communications made to or from the service would be likely to assist in connection with the investigation by the applicant agency of the following \*serious offence/\*serious offences, in which \*another person is/\*other persons are involved, with whom the \*particular person is/\*particular persons are likely to communicate using the service: [short particulars of the serious offence or serious offences]; and
  - (e) the warrant should be issued having regard to the following matters only:
    - (i) how much the privacy of any person or persons would be likely to be interfered with by intercepting, under a warrant, communications made to or from the service;
    - (ii) the gravity of the conduct constituting the \*offence/\*offences being investigated;
    - (iii) how much the information mentioned in paragraph (d) would be likely to assist in connection with the investigation by the applicant agency of the \*offence/\*offences;
    - (iv) to what extent methods of investigating the \*offence/\*offences that do not involve so intercepting communications have been used by, or are available to, the applicant agency;

- (v) how much the use of such methods would be likely to assist in connection with the investigation by the applicant agency of the \*offence/\*offences;
- (vi) how much the use of such methods would be likely to prejudice the investigation by the applicant agency of the \*offence/\*offences, whether because of delay or for any other reason;
- \*(vii) *[if the applicant agency is an interception agency of Victoria]* any submissions made by the Victorian PIM under section 44A of the Act to me;
- \*(viii) *[if the applicant agency is an interception agency of Queensland]* any submissions made by the Queensland PIM under section 45 of the Act to me.

(3) I am satisfied that:

\*the applicant agency has exhausted all other practicable methods of identifying the services used, or likely to be used, by the \*person/\*persons involved in the \*serious offence/\*serious offences being investigated.

\*interception of communications made to or from a service used or likely to be used by the particular \*person/\*persons involved in the \*serious offence/\*serious offences being investigated would not otherwise be possible.

2 Persons who may exercise this authority

Under subsection 55(1) of the Act, the authority conferred by this warrant may be exercised by an officer or staff member of the applicant agency, or another agency, in relation to whom an approval under subsection 55(3) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

3 Period for which warrant is in force

(1) Under section 54 of the Act, this warrant comes into force when it is issued.

(2) This warrant is in force until *[a date that is not more than 45 days away]*.

\*4 Conditions

Interceptions under this warrant are subject to the following conditions:  
*[details of conditions]*.

\*5 Restrictions

Interceptions under this warrant are subject to the following restrictions:  
*[details of restrictions]*.

Dated

.....  
\*Judge/\*nominated AAT member

\* Omit if not applicable

---

## Form 2A—Telecommunications service control order warrant

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

TELECOMMUNICATIONS SERVICE CONTROL ORDER WARRANT

<i>Telecommunications service</i>	[unique number assigned to the service; any other known unique identifying factors]
<i>Particular *person/*persons</i>	[full known *name/*names, other known names, other known identifying information (e.g. date of birth)]
<i>Applicant agency</i>	[name]

### 1 Authorisation

- (1) I, [name], \*an eligible Judge/\*a nominated AAT member within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 46 of the Act, authorise interceptions of communications made to or from the telecommunications service mentioned above.
- (2) I am satisfied, on the basis of the information given to me by the applicant agency, that:
  - (a) Division 3 of Part 2-5 of the Act has been complied with in relation to the application for this warrant; and
  - \* (b) because of urgent circumstances, it was necessary to make the application by telephone; and
  - (c) there are reasonable grounds for suspecting that the particular \*person/\*persons mentioned above \*is/\*are using, or \*is/\*are likely to use, the service; and
  - (d) \*a control order is/\*control orders are in force in relation to \*the particular person/\*each of the particular persons mentioned above; and
  - (e) information that would be likely to be obtained by intercepting under a warrant communications made to or from the service would be likely to substantially assist in connection with:
    - \* (i) the protection of the public from a terrorist act; or
    - \* (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - \* (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - \* (iv) determining whether the control \*order/\*orders, or any succeeding control \*order/\*orders, \*has/\*have been, or \*is/\*are being, complied with.
- (3) I am satisfied, on the basis of the information given to me by the applicant agency, that the warrant should be issued having regard to the following matters only:



- (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant communications made to or from the service;
  - (b) how much the information referred to in paragraph (2)(e) would be likely to assist in connection with:
    - (i) the protection of the public from a terrorist act; or
    - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - (iv) determining whether the control \*order/\*orders, or any succeeding control \*order/\*orders, \*has/\*have been, or \*is/\*are being, complied with;
  - (c) to what extent methods for:
    - (i) the protection of the public from a terrorist act; or
    - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - (iv) determining whether the control \*order/\*orders, or any succeeding control \*order/\*orders, \*has/\*have been, or \*is/\*are being, complied with;that do not involve so intercepting communications have been used by, or are available to, the applicant agency;
  - (d) how much the use of such methods would be likely to assist in connection with:
    - (i) the protection of the public from a terrorist act; or
    - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - (iv) determining whether the control \*order/\*orders, or any succeeding control \*order/\*orders, \*has/\*have been, or \*is/\*are being, complied with;
  - (e) how much the use of such methods would be likely to prejudice:
    - (i) the protection of the public from a terrorist act; or
    - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - (iv) determining whether the control \*order/\*orders, or any succeeding control \*order/\*orders, \*has/\*have been, or \*is/\*are being, complied with;whether because of delay or for any other reason;
  - (f) whether intercepting under a warrant communications made to or from the service would be the method that is likely to have the least interference with any person's privacy;
-

- (g) *\*[if the warrant is issued on the basis of more than one control order]* for each control order—  
the possibility that the person in relation to whom the control order is in force:
- (i) has engaged, is engaging, or will engage, in a terrorist act; or
  - (ii) has provided, is providing, or will provide, support for a terrorist act; or
  - (iii) has facilitated, is facilitating, or will facilitate, a terrorist act; or
  - (iv) has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country; or
  - (v) has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country; or
  - (vi) has contravened, is contravening, or will contravene, the control order; or
  - (vii) will contravene a succeeding control order;
- \*(h) [if the applicant agency is an interception agency of Victoria]* any submissions made by the Victorian PIM under section 44A of the Act to me;
- \*(i) [if the applicant agency is an interception agency of Queensland]* any submissions made by the Queensland PIM under section 45 of the Act to me.

- (4) This warrant is issued on the basis of the control *\*order/\*orders* mentioned in paragraph (2)(d), details of which are specified in the following table.

<b>Control <i>*order/*orders</i></b>		
<b>The name of the person in relation to whom the control order was made</b>	<b>The date the control order was made</b>	<b>Whether the control order is an interim control order or a confirmed control order</b>
<i>[the name of the person in relation to whom the control order was made]</i>	<i>[the date the control order was made]</i>	<i>*interim control order/* confirmed control order</i>

*[If the warrant is issued on the basis of more than one control order, include one item in the table for each control order.]*

## 2 Persons who may exercise this authority

Under subsection 55(1) of the Act, the authority conferred by this warrant may be exercised by a person in relation to whom an approval under subsection 55(3) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

## 3 Period for which warrant is in force

- (1) Under section 54 of the Act, this warrant comes into force when it is issued.
- (2) This warrant is in force until *[a date that is not more than 90 days away]*.

## *\*4* Conditions

Interceptions under this warrant are subject to the following conditions:

---

[*details of conditions*].

\*5 Restrictions

Interceptions under this warrant are subject to the following restrictions:

[*details of restrictions*].

Dated

.....  
\*Judge/\*nominated AAT member

\* Omit if not applicable

---

## Form 2B—Telecommunications service control order warrant—B-party

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

TELECOMMUNICATIONS SERVICE CONTROL ORDER WARRANT—B-PARTY

<i>Telecommunications service</i>	[unique number assigned to the service; any other known unique identifying factors]
<i>Particular *person/*persons</i>	[full known *name/*names, other known names, other known identifying information (e.g. date of birth)]
<i>Applicant agency</i>	[name]

### 1 Authorisation

- (1) I, [name], \*an eligible Judge/\*a nominated AAT member within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 46 of the Act, authorise interceptions of communications made to or from the telecommunications service mentioned above.
- (2) I am satisfied, on the basis of the information given to me by the applicant agency, that:
  - (a) Division 3 of Part 2-5 of the Act has been complied with in relation to the application for this warrant; and
  - \* (b) because of urgent circumstances, it was necessary to make the application by telephone; and
  - (c) there are reasonable grounds for suspecting that the particular \*person/\*persons mentioned above \*is/\*are using, or \*is/\*are likely to use, the service; and
  - (d) a control order is in force in relation to another person, and the particular \*person/\*persons mentioned above \*is/\*are likely to communicate with the other person using the service; and
  - (e) information that would be likely to be obtained by intercepting under a warrant communications made to or from the service would be likely to substantially assist in connection with:
    - \* (i) the protection of the public from a terrorist act; or
    - \* (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - \* (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - \* (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with.
- (3) I am satisfied, on the basis of the information given to me by the applicant agency, that the warrant should be issued having regard to the following matters only:

- 
- (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant communications made to or from the service;
- (b) how much the information referred to in paragraph (2)(e) would be likely to assist in connection with:
- (i) the protection of the public from a terrorist act; or
  - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
  - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
  - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;
- (c) to what extent methods for:
- (i) the protection of the public from a terrorist act; or
  - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
  - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
  - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;
- that do not involve so intercepting communications have been used by, or are available to, the applicant agency;
- (d) how much the use of such methods would be likely to assist in connection with:
- (i) the protection of the public from a terrorist act; or
  - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
  - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
  - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;
- (e) how much the use of such methods would be likely to prejudice:
- (i) the protection of the public from a terrorist act; or
  - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
  - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
  - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;
- whether because of delay or for any other reason;
- (f) whether intercepting under a warrant communications made to or from the service would be the method that is likely to have the least interference with any person's privacy;
- (g) the possibility that the person in relation to whom the control order is in force:
- (i) has engaged, is engaging, or will engage, in a terrorist act; or
-

**Schedule 1** Forms of warrants

**Form 2B** Telecommunications service control order warrant—B-party

- 
- (ii) has provided, is providing, or will provide, support for a terrorist act;  
or
- (iii) has facilitated, is facilitating, or will facilitate, a terrorist act; or
- (iv) has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country; or
- (v) has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country; or
- (vi) has contravened, is contravening, or will contravene, the control order; or
- (vii) will contravene a succeeding control order;
- <sup>\*</sup>(h) [*if the applicant agency is an interception agency of Victoria*] any submissions made by the Victorian PIM under section 44A of the Act to me;
- <sup>\*</sup>(i) [*if the applicant agency is an interception agency of Queensland*] any submissions made by the Queensland PIM under section 45 of the Act to me.
- (4) I am satisfied that:
- <sup>\*</sup>the applicant agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person to whom the control order relates.
- <sup>\*</sup>interception of communications made to or from a telecommunications service used or likely to be used by the person to whom the control order relates would not otherwise be possible.
- (5) This warrant is issued on the basis of the control order mentioned in paragraph (2)(d), details of which are specified in the following table.

---

<b>Control order</b>		
<b>The name of the person in relation to whom the control order was made</b>	<b>The date the control order was made</b>	<b>Whether the control order is an interim control order or a confirmed control order</b>
[ <i>the name of the person in relation to whom the control order was made</i> ]	[ <i>the date the control order was made</i> ]	<sup>*</sup> interim control order/ <sup>*</sup> confirmed control order

---

**2** Persons who may exercise this authority

Under subsection 55(1) of the Act, the authority conferred by this warrant may be exercised by a person in relation to whom an approval under subsection 55(3) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

**3** Period for which warrant is in force

- (1) Under section 54 of the Act, this warrant comes into force when it is issued.
- (2) This warrant is in force until [*a date that is not more than 45 days away*].
-

---

\*4 Conditions

Interceptions under this warrant are subject to the following conditions:  
[*details of conditions*].

\*5 Restrictions

Interceptions under this warrant are subject to the following restrictions:  
[*details of restrictions*].

Dated

.....  
\*Judge/\*nominated AAT member

\* Omit if not applicable

---

## Form 3—Named person warrant—telecommunications services

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

NAMED PERSON WARRANT — TELECOMMUNICATIONS SERVICES

<b>Particular person (named person)</b>	<i>[full known name, other known names, other known identifying information (e.g. date of birth)]</i>
---	---

<b>Applicant agency</b>	<i>[name]</i>
-------------------------	---------------

### 1 Authorisation

- (1) I, *[name]*, \*an eligible Judge/\*a nominated AAT member within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 46A of the Act, authorise interceptions of communications made to or from any telecommunications service that the named person mentioned above is using, or is likely to use.
- (2) I am satisfied, on the basis of the information given to me by the applicant agency, that:
- (a) Division 3 of Part 2-5 of the Act has been complied with in relation to the application for this warrant; and
  - \*(b) because of urgent circumstances, it was necessary to make the application by telephone; and
  - (c) there are reasonable grounds for suspecting that the named person is using, or is likely to use, more than 1 telecommunications service; and
  - (d) information that would be likely to be obtained by intercepting, under a warrant, communications made to or from any telecommunications service that the named person is using, or is likely to use, would be likely to assist in connection with the investigation by the agency of the following \*serious offence/ \*serious offences, in which the named person is involved:  
*[short particulars of the serious offence or serious offences]*; and
  - (e) the warrant should be issued having regard to the following matters only:
    - (i) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant, communications made to or from any telecommunications service used, or likely to be used, by the named person;
    - (ii) the gravity of the conduct constituting the \*offence/\*offences being investigated;
    - (iii) how much the information mentioned in paragraph (d) would be likely to assist in connection with the investigation by the applicant agency of the \*offence/\*offences;
    - (iv) to what extent methods (including the use of a warrant issued under section 46 of the Act) of investigating the \*offence/ \*offences that do not involve the use of a warrant issued under section 46A of the Act



---

in relation to the named person have been used by, or are available to, the applicant agency;

- (v) how much the use of such methods would be likely to assist in connection with the investigation by the applicant agency of the \*offence/\*offences;
- (vi) how much the use of such methods would be likely to prejudice the investigation by the applicant agency of the \*offence/\*offences, whether because of delay or for any other reason;
- \*(vii) *[if the applicant agency is an interception agency of Victoria]* any submissions made by the Victorian PIM under section 44A of the Act to me;
- \*(viii) *[if the applicant agency is an interception agency of Queensland]* any submissions made by the Queensland PIM under section 45 of the Act to me.

## 2 Persons who may exercise this authority

Under subsection 55 (1) of the Act, the authority conferred by this warrant may be exercised by an officer or staff member of the applicant agency, or another agency, in relation to whom an approval under subsection 55 (3) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

## 3 Period for which warrant is in force

- (1) Under section 54 of the Act, this warrant comes into force when it is issued.
- (2) This warrant is in force until *[a date that is not more than 90 days away]*.

## \*4 Conditions

Interceptions under this warrant are subject to the following conditions:  
*[details of conditions]*.

## \*5 Restrictions

### **\*General**

Interceptions under this warrant are subject to the following restrictions:  
*[details of restrictions]*.

### **\*Excluded telecommunications services**

This warrant does not authorise the interception of communications made to or from the following telecommunications services:  
*[details and location of service(s)]*.

Dated

.....  
\*Judge/\*nominated AAT member

**Schedule 1** Forms of warrants

**Form 3** Named person warrant—telecommunications services

---

\* Omit if not applicable

---

## Form 4—Named person warrant—telecommunications devices

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

NAMED PERSON WARRANT — TELECOMMUNICATIONS DEVICES

<b>Particular person</b> <b>(named person)</b>	[full known name, other known names, other known identifying information (e.g. date of birth)]
<b>Particular telecommunications</b> <b>*device/*devices</b>	[For each telecommunication device, the unique number assigned to the device (if known) and other known unique identifying factors]
<b>Applicant agency</b>	[name]

### 1 Authorisation

- (1) I, [name], \*an eligible Judge/\*a nominated AAT member within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 46A of the Act, authorise interceptions of communications made by means of the particular telecommunications \*device/\*devices that the named person mentioned above is using, or is likely to use.
- (2) I am satisfied, on the basis of the information given to me by the applicant agency, that:
  - (a) Division 3 of Part 2-5 of the Act has been complied with in relation to the application for this warrant; and
  - \*(b) because of urgent circumstances, it was necessary to make the application by telephone; and
  - (c) there are reasonable grounds for suspecting that the named person is using, or is likely to use, more than 1 telecommunications service; and
  - (d) information that would be likely to be obtained by intercepting, under a warrant, communications made by means of the particular telecommunications \*device/\*devices that the named person is using, or is likely to use, would be likely to assist in connection with the investigation by the agency of the following \*serious offence/\*serious offences, in which the named person is involved:  
[short particulars of the serious offence or serious offences]; and
  - (e) the warrant should be issued having regard to the following matters only:
    - (i) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant, communications made by means of the particular telecommunications \*device/\*devices used, or likely to be used, by the named person;
    - (ii) the gravity of the conduct constituting the \*offence/\*offences being investigated;

- 
- (iii) how much the information mentioned in paragraph (d) would be likely to assist in connection with the investigation by the applicant agency of the \*offence/\*offences;
  - (iv) to what extent methods (including the use of a warrant issued under section 46 of the Act) of investigating the \*offence/\*offences that do not involve the use of a warrant issued under section 46A of the Act in relation to the named person have been used by, or are available to, the applicant agency;
  - (v) how much the use of such methods would be likely to assist in connection with the investigation by the applicant agency of the \*offence/\*offences;
  - (vi) how much the use of such methods would be likely to prejudice the investigation by the applicant agency of the \*offence/\*offences, whether because of delay or for any other reason;
  - \*(vii) *[if the applicant agency is an interception agency of Victoria]* any submissions made by the Victorian PIM under section 44A of the Act to me;
  - \*(viii) *[if the applicant agency is an interception agency of Queensland]* any submissions made by the Queensland PIM under section 45 of the Act to me.

(3) I am satisfied that:

\*there are no other practicable methods available to the applicant agency at the time of making the application to identify the telecommunications services used, or likely to be used, by the named person.

\*interception of communications made to or from a telecommunications service used or likely to be used by the named person would not otherwise be practicable.

2 Persons who may exercise this authority

Under subsection 55(1) of the Act, the authority conferred by this warrant may be exercised by an officer or staff member of the applicant agency, or another agency, in relation to whom an approval under subsection 55(3) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

3 Period for which warrant is in force

(1) Under section 54 of the Act, this warrant comes into force when it is issued.

(2) This warrant is in force until *[a date that is not more than 90 days away]*.

\*4 Conditions

Interceptions under this warrant are subject to the following conditions:  
*[details of conditions]*.

\*5 Restrictions

Interceptions under this warrant are subject to the following restrictions:  
*[details of restrictions]*.

Dated

---

.....  
\*Judge/\*nominated AAT member

\* Omit if not applicable

---

## Form 4A—Named person control order warrant— telecommunications services

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

NAMED PERSON CONTROL ORDER WARRANT — TELECOMMUNICATIONS  
SERVICES

<b>Particular person (named person)</b>	<i>[full known name, other known names, other known identifying information (e.g. date of birth)]</i>
<b>Applicant agency</b>	<i>[name]</i>

---

### 1 Authorisation

- (1) I, *[name]*, \*an eligible Judge/\*a nominated AAT member within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 46A of the Act, authorise interceptions of communications made to or from any telecommunications service that the named person mentioned above is using, or is likely to use.
- (2) I am satisfied, on the basis of the information given to me by the applicant agency, that:
  - (a) Division 3 of Part 2-5 of the Act has been complied with in relation to the application for this warrant; and
  - \* (b) because of urgent circumstances, it was necessary to make the application by telephone; and
  - (c) there are reasonable grounds for suspecting that the named person is using, or is likely to use, more than 1 telecommunications service; and
  - (d) a control order is in force in relation to the named person; and
  - (e) information that would be likely to be obtained by intercepting under a warrant communications made to or from any telecommunications service that the named person is using, or is likely to use, would be likely to substantially assist in connection with:
    - \*(i) the protection of the public from a terrorist act; or
    - \*(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - \*(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - \*(iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with.
- (3) I am satisfied, on the basis of the information given to me by the applicant agency, that the warrant should be issued having regard to the following matters only:
  - (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant communications made to or

- 
- from any telecommunications service used, or likely to be used, by the named person;
- (b) how much the information referred to in paragraph (2)(e) would be likely to assist in connection with:
- (i) the protection of the public from a terrorist act; or
  - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
  - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
  - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;
- (c) to what extent methods (including the use of a warrant issued under section 46 of the Act) for:
- (i) the protection of the public from a terrorist act; or
  - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
  - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
  - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;
- that do not involve the use of a warrant issued under section 46A of the Act in relation to the named person have been used by, or are available to, the applicant agency;
- (d) how much the use of such methods would be likely to assist in connection with:
- (i) the protection of the public from a terrorist act; or
  - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
  - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
  - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;
- (e) how much the use of such methods would be likely to prejudice:
- (i) the protection of the public from a terrorist act; or
  - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
  - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
  - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;
- whether because of delay or for any other reason;
- (f) whether intercepting under a warrant communications referred to in paragraph (a) would be the method that is likely to have the least interference with any person's privacy;
- (g) the possibility that the named person:
- (i) has engaged, is engaging, or will engage, in a terrorist act; or
-

**Schedule 1** Forms of warrants

**Form 4A** Named person control order warrant—telecommunications services

- (ii) has provided, is providing, or will provide, support for a terrorist act; or
- (iii) has facilitated, is facilitating, or will facilitate, a terrorist act; or
- (iv) has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country; or
- (v) has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country; or
- (vi) has contravened, is contravening, or will contravene, the control order; or
- (vii) will contravene a succeeding control order;
- \* (h) *[if the applicant agency is an interception agency of Victoria]* any submissions made by the Victorian PIM under section 44A of the Act to me;
- \* (i) *[if the applicant agency is an interception agency of Queensland]* any submissions made by the Queensland PIM under section 45 of the Act to me.

- (4) This warrant is issued on the basis of the control order mentioned in paragraph (2)(d), details of which are specified in the following table.

<b>Control order</b>		
<b>The name of the person in relation to whom the control order was made</b>	<b>The date the control order was made</b>	<b>Whether the control order is an interim control order or a confirmed control order</b>
<i>[the name of the person in relation to whom the control order was made]</i>	<i>[the date the control order was made]</i>	*interim control order/*confirmed control order

**2** Persons who may exercise this authority

Under subsection 55(1) of the Act, the authority conferred by this warrant may be exercised by a person in relation to whom an approval under subsection 55(3) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

**3** Period for which warrant is in force

- (1) Under section 54 of the Act, this warrant comes into force when it is issued.
- (2) This warrant is in force until *[a date that is not more than 90 days away]*.

**\*4** Conditions

Interceptions under this warrant are subject to the following conditions:  
*[details of conditions]*.

**\*5** Restrictions

**\*General**

Interceptions under this warrant are subject to the following restrictions:  
*[details of restrictions]*.



---

**\*Excluded telecommunications services**

This warrant does not authorise the interception of communications made to or from the following telecommunications services:  
[*details and location of service(s)*].

Dated

.....  
\*Judge/\*nominated AAT member

\* Omit if not applicable

---

## Form 4B—Named person control order warrant— telecommunications devices

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

NAMED PERSON CONTROL ORDER WARRANT — TELECOMMUNICATIONS  
DEVICES

<b>Particular person</b> <b>(named person)</b>	<i>[full known name, other known names, other known identifying information (e.g. date of birth)]</i>
<b>Particular telecommunications</b> <b>*device/*devices</b>	<i>[For each telecommunication device, the unique number assigned to the device (if known) and other known unique identifying factors]</i>
<b>Applicant agency</b>	<i>[name]</i>

### 1 Authorisation

- (1) I, *[name]*, \*an eligible Judge/\*a nominated AAT member within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 46A of the Act, authorise interceptions of communications made by means of the particular telecommunications \*device/\*devices that the named person mentioned above is using, or is likely to use.
- (2) I am satisfied, on the basis of the information given to me by the applicant agency, that:
  - (a) Division 3 of Part 2-5 of the Act has been complied with in relation to the application for this warrant; and
  - \* (b) because of urgent circumstances, it was necessary to make the application by telephone; and
  - (c) there are reasonable grounds for suspecting that the named person is using, or is likely to use, more than 1 telecommunications service; and
  - (d) a control order is in force in relation to the named person; and
  - (e) information that would be likely to be obtained by intercepting under a warrant communications made by means of the particular telecommunications \*device/\*devices that the named person is using, or is likely to use, would be likely to substantially assist in connection with:
    - \*(i) the protection of the public from a terrorist act; or
    - \*(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - \*(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - \*(iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with.

- 
- (3) I am satisfied, on the basis of the information given to me by the applicant agency, that the warrant should be issued having regard to the following matters only:
- (a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant communications made by means of the particular telecommunications \*device/\*devices used, or likely to be used, by the named person;
  - (b) how much the information referred to in paragraph (2)(e) would be likely to assist in connection with:
    - (i) the protection of the public from a terrorist act; or
    - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;
  - (c) to what extent methods (including the use of a warrant issued under section 46 of the Act) for:
    - (i) the protection of the public from a terrorist act; or
    - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;that do not involve the use of a warrant issued under section 46A of the Act in relation to the named person have been used by, or are available to, the applicant agency;
  - (d) how much the use of such methods would be likely to assist in connection with:
    - (i) the protection of the public from a terrorist act; or
    - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;
  - (e) how much the use of such methods would be likely to prejudice:
    - (i) the protection of the public from a terrorist act; or
    - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
    - (iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
    - (iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with;whether because of delay or for any other reason;
-

**Schedule 1** Forms of warrants

**Form 4B** Named person control order warrant—telecommunications devices

- 
- (f) whether intercepting under a warrant communications referred to in paragraph (a) would be the method that is likely to have the least interference with any person's privacy;
- (g) the possibility that the named person:
- (i) has engaged, is engaging, or will engage, in a terrorist act; or
  - (ii) has provided, is providing, or will provide, support for a terrorist act; or
  - (iii) has facilitated, is facilitating, or will facilitate, a terrorist act; or
  - (iv) has provided, is providing, or will provide, support for the engagement in a hostile activity in a foreign country; or
  - (v) has facilitated, is facilitating, or will facilitate, the engagement in a hostile activity in a foreign country; or
  - (vi) has contravened, is contravening, or will contravene, the control order; or
  - (vii) will contravene a succeeding control order;
- <sup>\*</sup>(h) [*if the applicant agency is an interception agency of Victoria*] any submissions made by the Victorian PIM under section 44A of the Act to me;
- <sup>\*</sup>(i) [*if the applicant agency is an interception agency of Queensland*] any submissions made by the Queensland PIM under section 45 of the Act to me.
- (4) I am satisfied that:
- <sup>\*</sup>there are no other practicable methods available to the applicant agency at the time of making the application to identify the telecommunications services used, or likely to be used, by the named person.
  - <sup>\*</sup>interception of communications made to or from a telecommunications service used, or likely to be used, by the named person would not otherwise be practicable.
- (5) This warrant is issued on the basis of the control order mentioned in paragraph (2)(d), details of which are specified in the following table.

---

<b>Control order</b>		
<b>The name of the person in relation to whom the control order was made</b>	<b>The date the control order was made</b>	<b>Whether the control order is an interim control order or a confirmed control order</b>
[ <i>the name of the person in relation to whom the control order was made</i> ]	[ <i>the date the control order was made</i> ]	<sup>*</sup> interim control order/ <sup>*</sup> confirmed control order

---

**2 Persons who may exercise this authority**

Under subsection 55(1) of the Act, the authority conferred by this warrant may be exercised by a person in relation to whom an approval under subsection 55(3) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

---

3 Period for which warrant is in force

(1) Under section 54 of the Act, this warrant comes into force when it is issued.

(2) This warrant is in force until [*a date that is not more than 90 days away*].

\*4 Conditions

Interceptions under this warrant are subject to the following conditions:  
[*details of conditions*].

\*5 Restrictions

Interceptions under this warrant are subject to the following restrictions:  
[*details of restrictions*].

Dated

.....  
\*Judge/\*nominated AAT member

\* Omit if not applicable

---

## Form 5—Warrant for entry on premises and interception of communications

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

### WARRANT FOR ENTRY ON PREMISES AND INTERCEPTION OF COMMUNICATIONS

<b>Premises</b>	<i>[description and location of premises, including business name, operating name, other known names and other known identifying information]</i>
<b>Telecommunications service</b>	<i>[number assigned to the service; any other known unique identifying factors]</i>
<b>Particular person</b>	<i>[full known name, other known names, other known identifying information (e.g. date of birth)]</i>
<b>Applicant agency</b>	<i>[name]</i>

#### 1 Authorisation

- (1) I, *[name]*, \*an eligible Judge/\*a nominated AAT member within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 48 of the Act, authorise:
  - (a) entry on the premises mentioned above in order to install, maintain, use or recover equipment or a line used in the interception of communications being made to or from the telecommunications service mentioned above; and
  - (b) interceptions of such communications by the use of that equipment or line.
- (2) This warrant authorises:
  - (a) entry on the premises:
    - (i) \*at any time of the day or night/\*during the hours of *[specify hours during which entry on the premises is authorised]*, for the purposes mentioned in paragraph (1)(a); and
    - \*(ii) without permission first being sought or demand first being made; and
  - \*(b) the following measures, that I am satisfied are necessary and reasonable for those purposes:  
*[specify measures authorised to be taken]*.
- (3) I am satisfied:
  - (a) that subsection 48(2) of the Act has been complied with in relation to the application for this warrant; and
  - (b) on the basis of the information given to me by the applicant agency, that:
    - (i) section 46 of the Act would empower me to issue a warrant if the application had been made under that section; and

- 
- (ii) Division 3 of Part 2-5 of the Act has been complied with in relation to this application; and
- (iii) information that would be likely to be obtained by intercepting, under a warrant, communications made to or from the service, would be likely to assist in connection with the investigation by the applicant agency of the following \*serious offence/\*serious offences, in which \*the particular person mentioned above is involved:  
\*another person is involved, with whom the particular person mentioned above is likely to communicate using the service:  
[short particulars of the serious offence or serious offences]; and
- (c) on the basis of the information given to me by the applicant agency, that it would be impracticable or inappropriate to intercept communications under a warrant in respect of the service otherwise than by the use of equipment or a line installed on those premises:  
\*for technical reasons connected with the nature or operation of the service or of a telecommunications system of which the service forms a part.  
\*because, if the warrant were issued under section 46, communications to or from the telecommunications service would be intercepted while passing over a telecommunications system and execution of the warrant as a result of action taken by employees of that carrier might jeopardise the security of the investigation, by the applicant agency, of a serious offence in which a person to whom the application relates is involved.

2 Persons who may exercise this authority

Under subsection 55(1) of the Act, the authority conferred by this warrant applies to an officer or staff member of the applicant agency, or another agency, in relation to whom an approval under subsection 55(3) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

3 Period for which warrant is in force

- (1) Under section 54 of the Act, this warrant comes into force when it is issued.
- (2) This warrant is in force until [specify date].  
[specify a date that is:  
(a) if subparagraph 46(1)(d)(ii) of the Act would apply if the application had been made under section 46 of the Act — not more than 45 days away; or  
(b) otherwise — not more than 90 days away]

\*4 Conditions

Interceptions under this warrant are subject to the following conditions:  
[details of conditions].

\*5 Restrictions

Interceptions under this warrant are subject to the following restrictions:  
[details of restrictions].

**Schedule 1** Forms of warrants

**Form 5** Warrant for entry on premises and interception of communications

---

Dated

.....  
\*Judge/\*nominated AAT member

\* Omit if not applicable



---

## **Form 5A—Control order warrant for entry on premises and interception of communications**

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

CONTROL ORDER WARRANT FOR ENTRY ON PREMISES AND INTERCEPTION OF COMMUNICATIONS

<b>Premises</b>	<i>[description and location of premises, including business name, operating name, other known names and other known identifying information]</i>
<b>Telecommunications service</b>	<i>[number assigned to the service; any other known unique identifying factors]</i>
<b>Particular person</b>	<i>[full known name, other known names, other known identifying information (e.g. date of birth)]</i>
<b>Applicant agency</b>	<i>[name]</i>

### 1 Authorisation

- (1) I, *[name]*, \*an eligible Judge/\*a nominated AAT member within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 48 of the Act, authorise:
- (a) entry on the premises mentioned above in order to install, maintain, use or recover equipment or a line used in the interception of communications being made to or from the telecommunications service mentioned above; and
  - (b) interceptions of such communications by the use of that equipment or line.
- (2) This warrant authorises:
- (a) entry on the premises:
    - (i) \*at any time of the day or night/\*during the hours of *[specify hours during which entry on the premises is authorised]*, for the purposes mentioned in paragraph (1)(a); and
    - \*(ii) without permission first being sought or demand first being made; and
  - \*(b) the following measures, that I am satisfied are necessary and reasonable for those purposes:  
*[specify measures authorised to be taken]*.
- (3) I am satisfied:
- (a) that subsection 48(2) of the Act has been complied with in relation to the application for this warrant; and
  - (b) on the basis of the information given to me by the applicant agency, that:
    - (i) subsection 46(4) of the Act would empower me to issue a warrant if the application had been made under that section; and

**Schedule 1** Forms of warrants

**Form 5A** Control order warrant for entry on premises and interception of communications

- 
- (ii) Division 3 of Part 2-5 of the Act has been complied with in relation to this application; and
- (iii) a control order is in force in relation to:
- \*[if subparagraph 46(4)(d)(ii) of the Act would apply if the application had been made under section 46 of the Act] the particular person mentioned above; and
- \*[otherwise] a person other than the particular person mentioned above, and the particular person mentioned above is likely to communicate with the other person using the service; and
- (c) on the basis of the information given to me by the applicant agency, that information that would be likely to be obtained by intercepting under a warrant communications made to or from the service would be likely to substantially assist in connection with:
- \*(i) the protection of the public from a terrorist act; or
- \*(ii) preventing the provision of support for, or the facilitation of, a terrorist act; or
- \*(iii) preventing the provision of support for, or the facilitation of, the engagement in a hostile activity in a foreign country; or
- \*(iv) determining whether the control order, or any succeeding control order, has been, or is being, complied with; and
- (d) on the basis of the information given to me by the applicant agency, that it would be impracticable or inappropriate to intercept communications under a warrant in respect of the service otherwise than by the use of equipment or a line installed on those premises:
- \*for technical reasons connected with the nature or operation of the service or of a telecommunications system of which the service forms a part.
- \*because, if the warrant were issued under section 46, communications to or from the telecommunications service would be intercepted while passing over a telecommunications system and execution of the warrant as a result of action taken by employees of that carrier might jeopardise the achievement of the objective for which the warrant was issued.
- (4) This warrant is issued on the basis of the control order mentioned in subparagraph (3)(b)(iii), details of which are specified in the following table.

---

<b>Control order</b>		
<b>The name of the person in relation to whom the control order was made</b>	<b>The date the control order was made</b>	<b>Whether the control order is an interim control order or a confirmed control order</b>
<i>[the name of the person in relation to whom the control order was made]</i>	<i>[the date the control order was made]</i>	*interim control order/*confirmed control order

---

2 Persons who may exercise this authority

Under subsection 55(1) of the Act, the authority conferred by this warrant applies to a person in relation to whom an approval under subsection 55(3) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

3 Period for which warrant is in force

(1) Under section 54 of the Act, this warrant comes into force when it is issued.

(2) This warrant is in force until [*specify date*].

[*specify a date that is:*

(a) *if subparagraph 46(4)(d)(ii) of the Act would apply if the application had been made under section 46 of the Act—not more than 45 days away; or*

(b) *otherwise—not more than 90 days away]*

\*4 Conditions

Interceptions under this warrant are subject to the following conditions:

[*details of conditions*].

\*5 Restrictions

Interceptions under this warrant are subject to the following restrictions:

[*details of restrictions*].

Dated

.....  
\*Judge/\*nominated AAT member

\* Omit if not applicable

---

## Form 6—Stored communications warrant—domestic

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

### STORED COMMUNICATIONS WARRANT

<b>Person in respect of whom warrant is issued</b>	[full known name, other known names, other known identifying information (e.g. date of birth)]
--	---

<b>Applicant criminal law-enforcement agency</b>	[name]
--	--------

<b>Person making application on behalf of applicant criminal law-enforcement agency</b>	[full name]
---	-------------

Note: See subsections 119(4) and (5) of the Act in relation to issuing a further warrant in respect of a person in respect of whom a previous warrant was issued.

#### 1 Authorisation

- (1) I, [name], an issuing authority within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 116 of the Act, authorise the accessing of any stored communication:
  - (a) that was made by the person mentioned above, or that another person has made and for which the intended recipient is the person mentioned above; and
  - (b) that becomes, or became, a stored communication before the warrant is first executed in relation to the carrier that holds the communication.
- (2) I am satisfied, on the basis of the information given to me under Part 3-3 of the Act in connection with the application for this warrant, that:
  - (a) Division 1 of Part 3-3 of the Act has been complied with in relation to the application for this warrant; and
  - \*(b) because of urgent circumstances, it was necessary to make the application by telephone; and
  - (c) there are reasonable grounds for suspecting that \*a particular carrier holds/\*particular carriers hold stored communications:
    - (i) that the person mentioned above has made; or
    - (ii) that another person has made and for which the person mentioned above is the intended recipient; and
  - (d) information that would be likely to be obtained by accessing those stored communications under a stored communications warrant would be likely to assist in connection with the investigation by the applicant criminal law-enforcement agency of the following \*serious contravention/\*serious contraventions in which the person mentioned above is involved:  
[short particulars of each serious contravention]; and
  - \*(e) the person mentioned above is a victim of a serious contravention and:
    - (i) the person is unable to consent; or

- 
- (ii) it is impracticable for the person to consent;  
to those stored communications being accessed; and
  - (f) the warrant should be issued having regard to the following matters only:
    - (i) how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant;
    - (ii) the gravity of the conduct constituting each serious contravention;
    - (iii) how much the information referred to in paragraph (d) would be likely to assist in connection with the investigation by the applicant criminal law-enforcement agency of each serious contravention;
    - (iv) to what extent the methods of investigating each serious contravention that do not involve the use of a stored communications warrant in relation to the person mentioned above have been used by, or are available to, the applicant criminal law-enforcement agency;
    - (v) how much the use of such methods would be likely to assist in connection with the investigation by the applicant criminal law-enforcement agency of each serious contravention;
    - (vi) how much the use of such methods would be likely to prejudice the investigation by the applicant criminal law-enforcement agency of each serious contravention, whether because of delay or for any other reason.

## 2 Persons who may exercise this authority

Under section 127 of the Act, the authority conferred by this warrant may be exercised by an officer or staff member of the applicant criminal law-enforcement agency, or another criminal law-enforcement agency, in relation to whom an approval under subsection 127(2) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

## 3 Duration of warrant

- (1) Under section 125 of the Act, this warrant comes into force when it is issued.
- \*(2) Under subsection 119(1) of the Act, this warrant remains in force until the occurrence of the sooner of the following:
  - (a) the warrant is first executed;
  - (b) the end of the period of 5 days after the day on which it was issued.

*[Complete the above subclause only if the warrant relates to 1 or more telecommunication services that are all operated by the same carrier]*

- \*(2) Under subsection 119(2) of the Act, this warrant remains in force, to the extent that it relates to a telecommunications service operated by a particular carrier, until the occurrence of the sooner of the following:
  - (a) the warrant is first executed in relation to a telecommunications service operated by that particular carrier;
  - (b) the end of the period of 5 days after the day on which it was issued.

*[Complete the above subclause only if the warrant relates to 2 or more telecommunications services that are not all operated by the same carrier]*

**Schedule 1** Forms of warrants

**Form 6** Stored communications warrant—domestic

---

\*4 Conditions

The accessing of stored communications under this warrant is subject to the following conditions:  
[*details of conditions*].

\*5 Restrictions

The accessing of stored communications under this warrant is subject to the following restrictions:  
[*details of restrictions*].

Dated

.....  
Issuing Authority

\* Omit if not applicable

---

## Form 6A—Stored communications warrant—international

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*  
STORED COMMUNICATIONS WARRANT

---

<b>Person in respect of whom warrant is issued</b>	[full known name, other known names, other known identifying information (e.g. date of birth)]
--	--

---

<b>Applicant criminal law-enforcement agency</b>	[name]
--	--------

---

<b>Person making application on behalf of applicant criminal law-enforcement agency</b>	[full name]
---	-------------

---

Note: See subsections 119(4) and (5) of the Act in relation to issuing a further warrant in respect of a person in respect of whom a previous warrant was issued.

### 1 Authorisation

- (1) I, [name], an issuing authority within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 116 of the Act, authorise the accessing of any stored communication:
  - (a) that was made by the person mentioned above, or that another person has made and for which the intended recipient is the person mentioned above; and
  - (b) that becomes, or became, a stored communication before the warrant is first executed in relation to the carrier that holds the communication.
- (2) I am satisfied, on the basis of the information given to me under Part 3-3 of the Act in connection with the application for this warrant, that:
  - (a) Division 1 of Part 3-3 of the Act has been complied with in relation to the application for this warrant; and
  - \*(b) because of urgent circumstances, it was necessary to make the application by telephone; and
  - (c) there are reasonable grounds for suspecting that \*a particular carrier holds/\*particular carriers hold stored communications:
    - (i) that the person mentioned above has made; or
    - (ii) that another person has made and for which the person mentioned above is the intended recipient; and
  - (d) information that would be likely to be obtained by accessing those stored communications under a stored communications warrant would be likely to assist in connection with the investigation, investigative proceeding, or proceeding by [name of entity to which the application relates], of the following \*serious foreign contravention/\*serious foreign contraventions in which the person mentioned above is involved:  
[short particulars of each serious foreign contravention]; and
  - (e) the warrant should be issued having regard to the following matters only:

- 
- (i) how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant;
  - (ii) the gravity of the conduct constituting each serious foreign contravention;
  - (iii) how much the information referred to in paragraph (d) would be likely to assist in connection with the investigation, investigative proceeding, or proceeding by [*name of entity to which the application relates*], of each serious foreign contravention, to the extent that this is possible to determine from information obtained from [*name of entity to which the application relates*].

## 2 Persons who may exercise this authority

Under section 127 of the Act, the authority conferred by this warrant may be exercised by an officer or staff member of the applicant criminal law-enforcement agency, or another criminal law-enforcement agency, in relation to whom an approval under subsection 127(2) of the Act is in force in relation to the warrant, or to the class of warrants to which it belongs.

## 3 Duration of warrant

(1) Under section 125 of the Act, this warrant comes into force when it is issued.

\*(2) Under subsection 119(1) of the Act, this warrant remains in force until the occurrence of the sooner of the following:

- (a) the warrant is first executed;
- (b) the end of the period of 5 days after the day on which it was issued.

[*Complete the above subclause only if the warrant relates to 1 or more telecommunication services that are all operated by the same carrier*]

\*(2) Under subsection 119(2) of the Act, this warrant remains in force, to the extent that it relates to a telecommunications service operated by a particular carrier, until the occurrence of the sooner of the following:

- (a) the warrant is first executed in relation to a telecommunications service operated by that particular carrier;
- (b) the end of the period of 5 days after the day on which it was issued.

[*Complete the above subclause only if the warrant relates to 2 or more telecommunications services that are not all operated by the same carrier*]

## \*4 Conditions

The accessing of stored communications under this warrant is subject to the following conditions:  
[*details of conditions*].

## \*5 Restrictions

The accessing of stored communications under this warrant is subject to the following restrictions:  
[*details of restrictions*].



---

Dated

.....  
Issuing Authority

\* Omit if not applicable

---

## Form 7—Journalist information warrant

Commonwealth of Australia

*Telecommunications (Interception and Access) Act 1979*

JOURNALIST INFORMATION WARRANT

<i>*Person/*persons in respect of whom warrant is issued</i>	<i>[full known name, other known names, other known identifying information (e.g. date of birth or Australian Business Number)]</i>
--	---

<i>Applicant enforcement agency</i>	<i>[name]</i>
-------------------------------------	---------------

<i>Person making application on behalf of applicant enforcement agency</i>	<i>[full name]</i>
--	--------------------

Note: See subsection 180U(5) of the Act in relation to issuing a further warrant in relation to a person or persons in respect of whom a warrant has, or warrants have, previously been issued.

### 1 Authorisation

- (1) I, *[name]*, a Part 4-1 issuing authority within the meaning of the *Telecommunications (Interception and Access) Act 1979* (the **Act**), acting under section 180T of the Act, authorise the making of one or more authorisations under *\*section/\*sections* 178, 178A, 179 or 180 of the Act in relation to the particular *\*person/\*persons* mentioned above.
- (2) I am satisfied, on the basis of the information given to me by the applicant enforcement agency, that:
  - (a) this warrant is reasonably necessary for the following *\*purpose/\*purposes*:
    - \*(i) [if the warrant authorises the making of authorisations under section 178 of the Act]* for the enforcement of the criminal law;
    - \*(ii) [if the warrant authorises the making of authorisations under section 178A of the Act]* to find a person who the Australian Federal Police, or a Police Force of a State, has been notified is missing;
    - \*(iii) [if the warrant authorises the making of authorisations under section 179 of the Act]* for the enforcement of a law imposing a pecuniary penalty or the protection of the public revenue;
    - \*(iv) [if the warrant authorises the making of authorisations under section 180 of the Act]* the investigation of an offence of a kind referred to in subsection 180(4) of the Act; and
  - (b) the public interest in issuing this warrant outweighs the public interest in protecting the confidentiality of the source in connection with whom authorisations would be made, having regard to the matters set out in paragraph 180T(2)(b) of the Act.  
*\*[short particulars of each other matter to which regard was had, as allowed by subparagraph 180T(2)(b)(vi) of the Act].*

### 2 Persons who may exercise this authority

The authority conferred by this warrant may be exercised by an authorised officer of the applicant enforcement agency.

---

3 Duration of warrant

- (1) Under section 180V of the Act, this warrant comes into force when it is issued.
- (2) Under subsection 180U(3) of the Act, this warrant remains in force until [*a date that is not more than 90 days away*].

\*4 Conditions

The making of an authorisation under this warrant is subject to the following conditions:

[*details of conditions*].

\*5 Restrictions

The making of an authorisation under this warrant is subject to the following restrictions:

[*details of restrictions*].

Dated

.....  
Part 4-1 Issuing Authority

\* Omit if not applicable

## Endnotes

### Endnote 1—About the endnotes

---

## 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 the amendment to be made. If, despite the misdescription, the amendment can be given effect as intended, the amendment is incorporated into the compiled law and the abbreviation “(md)” added to the details of the amendment included in the amendment history.

If a misdescribed amendment cannot be given effect as intended, the abbreviation “(md not incorp)” is added to the details of the amendment included in the amendment history.

**Endnote 2—Abbreviation key**

ad = added or inserted	o = order(s)
am = amended	Ord = Ordinance
amdt = amendment	orig = original
c = clause(s)	par = paragraph(s)/subparagraph(s) /sub-subparagraph(s)
C[x] = Compilation No. x	pres = present
Ch = Chapter(s)	prev = previous
def = definition(s)	(prev...) = previously
Dict = Dictionary	Pt = Part(s)
disallowed = disallowed by Parliament	r = regulation(s)/rule(s)
Div = Division(s)	reloc = relocated
ed = editorial change	renum = renumbered
exp = expires/expired or ceases/ceased to have effect	rep = repealed
F = Federal Register of Legislation	rs = repealed and substituted
gaz = gazette	s = section(s)/subsection(s)
LA = <i>Legislation Act 2003</i>	Sch = Schedule(s)
LIA = <i>Legislative Instruments Act 2003</i>	Sdiv = Subdivision(s)
(md) = misdescribed amendment can be given effect	SLI = Select Legislative Instrument
(md not incorp) = misdescribed amendment cannot be given effect	SR = Statutory Rules
mod = modified/modification	Sub-Ch = Sub-Chapter(s)
No. = Number(s)	SubPt = Subpart(s)
	<u>underlining</u> = whole or part not commenced or to be commenced

## Endnotes

### Endnote 3—Legislation history

---

#### Endnote 3—Legislation history

Name	Registration	Commencement	Application, saving and transitional provisions
Telecommunications (Interception and Access) Regulations 2017	21 Dec 2017 (F2017L01701)	22 Dec 2017 (s 2(1) item 1)	
Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Regulations 2018	8 Oct 2018 (F2018L01408)	Sch 1 (items 4, 5): 22 Nov 2018 (s 2(1) item 2)	—
Telecommunications (Interception and Access) Amendment (Form of Warrants) Regulations 2019	21 Feb 2019 (F2019L00161)	22 Feb 2019 (s 2(1) item 1)	—
Telecommunications (Interception and Access) Amendment Regulations 2019	22 Feb 2019 (F2019L00162)	23 Feb 2019 (s 2(1) item 1)	—
Telecommunications (Interception and Access) Amendment (Form of Warrants No. 2) Regulations 2019	2 Dec 2019 (F2019L01552)	3 Dec 2019 (s 2(1) item 1)	—

## Endnote 4—Amendment history

## Endnote 4—Amendment history

Provision affected	How affected
<b>Part 1</b>	
s 2 .....	rep LA s 48D
s 4 .....	rep LA s 48C
<b>Part 2</b>	
s 6 .....	ed C3
s 7 .....	ed C3
s 8 .....	am F2019L00161
s 9 .....	rs F2018L01408
<b>Part 3</b>	
<b>Division 1</b>	
s 13 .....	am F2019L00162
s 14 .....	am F2019L00162
s 16 .....	am F2019L00162
s 17 .....	am F2019L00162
<b>Division 2</b>	
s 21 .....	am F2019L00162
<b>Schedule 1</b>	
Form 1 .....	am F2019L01552
Form 2 .....	am F2019L01552
Form 2A .....	ad F2019L00161
Form 2B.....	ad F2019L00161
Form 3 .....	am F2019L01552
Form 4 .....	am F2019L01552
Form 4A .....	ad F2019L00161
Form 4B.....	ad F2019L00161
Form 5A .....	ad F2019L00161
Form 6 .....	rs F2018L01408
Form 6A .....	ad F2018L01408
Schedule 2 .....	rep LA s 48C