

2019-2020-2021

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

As passed by both Houses

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021

No. , 2021

**A Bill for an Act to amend the *Surveillance Devices
Act 2004*, and for other purposes**

Contents

| | | |
|---|---|-----|
| 1 | Short title..... | 1 |
| 2 | Commencement..... | 1 |
| 3 | Schedules..... | 2 |
| Schedule 1—Data disruption | | 3 |
| | <i>Surveillance Devices Act 2004</i> | 3 |
| | <i>Telecommunications (Interception and Access) Act 1979</i> | 42 |
| Schedule 2—Network activity warrants | | 48 |
| Part 1—Main amendments | | 48 |
| | <i>Surveillance Devices Act 2004</i> | 48 |
| Part 2—Consequential amendments | | 81 |
| | <i>Australian Crime Commission Act 2002</i> | 81 |
| | <i>Australian Federal Police Act 1979</i> | 81 |
| | <i>Australian Human Rights Commission Act 1986</i> | 82 |
| | <i>Australian Information Commissioner Act 2010</i> | 85 |
| | <i>Inspector-General of Intelligence and Security Act 1986</i> | 85 |
| | <i>Law Enforcement Integrity Commissioner Act 2006</i> | 95 |
| | <i>Ombudsman Act 1976</i> | 97 |
| | <i>Privacy Act 1988</i> | 100 |
| | <i>Public Interest Disclosure Act 2013</i> | 101 |
| | <i>Telecommunications (Interception and Access) Act 1979</i> | 104 |
| Schedule 3—Account takeover warrants | | 109 |
| | <i>Crimes Act 1914</i> | 109 |
| | <i>National Emergency Declaration Act 2020</i> | 152 |
| Schedule 3A—Reviews | | 153 |
| | <i>Independent National Security Legislation Monitor Act 2010</i> | 153 |
| | <i>Intelligence Services Act 2001</i> | 153 |
| Schedule 4—Controlled operations | | 154 |
| | <i>Crimes Act 1914</i> | 154 |
| Schedule 5—Minor amendments | | 155 |

| | |
|--|-----|
| <i>Surveillance Devices Act 2004</i> | 155 |
| <i>Telecommunications (Interception and Access) Act 1979</i> | 155 |

1 **A Bill for an Act to amend the *Surveillance Devices***
2 ***Act 2004, and for other purposes***

3 The Parliament of Australia enacts:

4 **1 Short title**

5 This Act is the *Surveillance Legislation Amendment (Identify and*
6 *Disrupt) Act 2021*.

7 **2 Commencement**

8 (1) Each provision of this Act specified in column 1 of the table
9 commences, or is taken to have commenced, in accordance with
10 column 2 of the table. Any other statement in column 2 has effect
11 according to its terms.
12

Schedule 1—Data disruption

Surveillance Devices Act 2004

1 Title

After “access to”, insert “, and disruption of,”.

2 After paragraph 3(aaa)

Insert:

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

- (i) authorise the disruption of data held in computers; and
- (ii) are likely to substantially assist in frustrating the commission of relevant offences; and

3 Paragraph 3(ba)

After “accessing”, insert “or disrupting”.

4 Paragraph 3(ba)

After “operations”, insert “or computer data disruption operations”.

5 Paragraph 3(c)

Omit “and computer data access operations”, substitute “, computer data access operations and computer data disruption operations”.

6 At the end of subsection 4(1)

Add:

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

7 After subsection 4(4A)

Insert:

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

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

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

8 Subsection 6(1)

Insert:

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

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

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

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

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

- (a) data disruption warrants; or
- (b) emergency authorisations for disruption of data held in a computer.

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

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

IGIS official means:

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

Ombudsman official means:

- (a) the Ombudsman; or
- (b) a Deputy Commonwealth Ombudsman; or
- (c) a person who is a member of the staff referred to in subsection 31(1) of the *Ombudsman Act 1976*.

9 Subsection 6(1) (definition of remote application)

Omit “or 27B”, substitute “, 27B or 27KB”.

10 Subsection 6(1) (definition of *unsworn application*)

Omit “or 27A(13) and (14)”, substitute “, 27A(13) and (14) or 27KA(4) and (5)”.

11 Subsection 6(1) (at the end of the definition of *warrant*)

Add:
; or (d) a data disruption warrant.

12 At the end of subsection 10(1)

Add:
; (d) a data disruption warrant.

13 At the end of Part 2

Add:

Division 5—Data disruption warrants

27KAA Sunsetting

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

27KA Application for data disruption warrant

- (1) A law enforcement officer of the Australian Federal Police or the Australian Crime Commission (or another person on the law enforcement officer’s behalf) may apply for the issue of a data disruption warrant if the law enforcement officer suspects on reasonable grounds that:
 - (a) one or more relevant offences of a particular kind have been, are being, are about to be, or are likely to be, committed; and
 - (b) those offences involve, or are likely to involve, data held in a computer (the *target computer*); and
 - (c) disruption of data held in the target computer is likely to substantially assist in frustrating the commission of one or more relevant offences that:
 - (i) involve, or are likely to involve, data held in the target computer; and

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

3 *Procedure for making applications*

- 4 (2) An application under subsection (1) may be made to an eligible
5 Judge or to a nominated AAT member.
- 6 (3) An application:
7 (a) must specify:
8 (i) the name of the applicant; and
9 (ii) the nature and duration of the warrant sought; and
10 (b) subject to this section, must be supported by an affidavit
11 setting out:
12 (i) the grounds on which the warrant is sought; and
13 (ii) the things proposed to be authorised by the warrant in
14 accordance with section 27KE; and
15 (iii) an assessment of how disruption of data held in the
16 target computer is likely to substantially assist as
17 described in paragraph (1)(c), to the extent that such an
18 assessment is possible; and
19 (iv) an assessment of the likelihood that disruption of data
20 held in the target computer will substantially assist as
21 described in paragraph (1)(c), to the extent that such an
22 assessment is possible.

23 *Unsworn applications*

- 24 (4) If a law enforcement officer believes that:
25 (a) immediate disruption of data held in the target computer
26 referred to in subsection (1) is likely to substantially assist as
27 described in paragraph (1)(c); and
28 (b) it is impracticable for an affidavit to be prepared or sworn
29 before an application for a warrant is made;
30 an application for a warrant under subsection (1) may be made
31 before an affidavit is prepared or sworn.
- 32 (5) If subsection (4) applies, the applicant must:

-
- (a) provide as much information as the eligible Judge or nominated AAT member considers is reasonably practicable in the circumstances; and
 - (b) not later than 72 hours after the making of the application, send a duly sworn affidavit to the eligible Judge or nominated AAT member, whether or not a warrant has been issued.

Target computer

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

27KB Remote application

- (1) If a law enforcement officer believes that it is impracticable for an application for a data disruption warrant to be made in person, the application may be made under section 27KA by telephone, fax, email or any other means of communication.
- (2) If transmission by fax is available and an affidavit has been prepared, the person applying must transmit a copy of the affidavit, whether sworn or unsworn, to the eligible Judge or to the nominated AAT member who is to determine the application.

27KBA Endorsement of application—Australian Federal Police

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

- 1 disruption warrant unless the endorsing officer is satisfied that the
2 making of the application is appropriate in all the circumstances.
- 3 (3) For the purposes of this section, an **endorsing officer** of the
4 Australian Federal Police means:
- 5 (a) a law enforcement officer of the Australian Federal Police
6 who is declared, in writing, by the chief officer of the
7 Australian Federal Police to be an endorsing officer of the
8 Australian Federal Police; or
- 9 (b) a person who is in a class of law enforcement officers of the
10 Australian Federal Police that is declared, in writing, by the
11 chief officer of the Australian Federal Police to be a class of
12 endorsing officers of the Australian Federal Police.
- 13 (4) The chief officer of the Australian Federal Police must not make a
14 declaration under paragraph (3)(a) in relation to a law enforcement
15 officer of the Australian Federal Police unless:
- 16 (a) the law enforcement officer is a superintendent, or a person
17 holding a higher rank, in the Australian Federal Police; and
- 18 (b) the chief officer is satisfied that the law enforcement officer
19 has the relevant skills, knowledge and experience to endorse
20 the making of applications for the issue of data disruption
21 warrants; and
- 22 (c) the chief officer is satisfied that the law enforcement officer
23 has completed all current internal training requirements
24 relating to endorsing the making of applications for the issue
25 of data disruption warrants.
- 26 (5) The chief officer of the Australian Federal Police must not make a
27 declaration under paragraph (3)(b) in relation to a class of law
28 enforcement officers of the Australian Federal Police unless:
- 29 (a) each person in that class is a superintendent, or a person
30 holding a higher rank, in the Australian Federal Police; and
- 31 (b) the chief officer is satisfied that each person in that class has
32 the relevant skills, knowledge and experience to endorse the
33 making of applications for the issue of data disruption
34 warrants; and
- 35 (c) the chief officer is satisfied that each person in that class has
36 completed all current internal training requirements relating

to endorsing the making of applications for the issue of data
disruption warrants.

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

27KBB Endorsement of application—Australian Crime Commission

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

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

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

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

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

- (a) the law enforcement officer is an executive level member of the staff of the Australian Crime Commission; and
- (b) the chief officer is satisfied that the law enforcement officer has the relevant skills, knowledge and experience to endorse the making of applications for the issue of data disruption warrants; and

- 1 (c) the chief officer is satisfied that the law enforcement officer
2 has completed all current internal training requirements
3 relating to endorsing the making of applications for the issue
4 of data disruption warrants.
- 5 (5) The chief officer of the Australian Crime Commission must not
6 make a declaration under paragraph (3)(b) in relation to a class of
7 law enforcement officers of the Australian Crime Commission
8 unless:
- 9 (a) each person in that class is an executive level member of the
10 staff of the Australian Crime Commission; and
- 11 (b) the chief officer is satisfied that each person in that class has
12 the relevant skills, knowledge and experience to endorse the
13 making of applications for the issue of data disruption
14 warrants; and
- 15 (c) the chief officer is satisfied that each person in that class has
16 completed all current internal training requirements relating
17 to endorsing the making of applications for the issue of data
18 disruption warrants.
- 19 (6) A declaration under this section is not a legislative instrument.

20 **27KC Determining the application**

- 21 (1) An eligible Judge or a nominated AAT member may issue a data
22 disruption warrant if satisfied:
- 23 (a) that there are reasonable grounds for the suspicion founding
24 the application for the warrant; and
- 25 (b) the disruption of data authorised by the warrant is reasonably
26 necessary and proportionate, having regard to the offences
27 referred to in paragraph 27KA(1)(c); and
- 28 (c) in the case of an unsworn application—that it would have
29 been impracticable for an affidavit to have been sworn or
30 prepared before the application was made; and
- 31 (d) in the case of a remote application—that it would have been
32 impracticable for the application to have been made in
33 person.
- 34 (2) In determining whether a data disruption warrant should be issued,
35 the eligible Judge or nominated AAT member must have regard to:

-
- 1 (a) the nature and gravity of the conduct constituting the
2 offences referred to in paragraph 27KA(1)(c); and
3 (b) the likelihood that the disruption of data authorised by the
4 warrant will frustrate the commission of the offences referred
5 to in paragraph 27KA(1)(c); and
6 (c) the existence of any alternative means of frustrating the
7 commission of the offences referred to in
8 paragraph 27KA(1)(c); and
9 (ca) the nature of the things proposed to be authorised by the
10 warrant in accordance with section 27KE; and
11 (cb) the extent to which the execution of the warrant is likely to
12 result in access to, or disruption of, data of persons lawfully
13 using a computer, and any privacy implications (to the extent
14 known) resulting from that access or disruption; and
15 (cc) any steps that are proposed to be taken to avoid or minimise
16 the extent to which the execution of the warrant is likely to
17 impact on persons lawfully using a computer; and
18 (cd) the extent to which the execution of the warrant is likely to
19 cause a person to suffer a temporary loss of:
20 (i) money; or
21 (ii) digital currency; or
22 (iii) property (other than data);
23 so far as that matter is known to the eligible Judge or
24 nominated AAT member; and
25 (ce) if:
26 (i) the eligible Judge or nominated AAT member believes
27 on reasonable grounds that the data covered by the
28 warrant (within the meaning of section 27KE) is data of
29 a person who is working in a professional capacity as a
30 journalist or of an employer of such a person; and
31 (ii) each of the offences referred to in
32 paragraph 27KA(1)(c) is an offence against a secrecy
33 provision;
34 whether the public interest in issuing the warrant outweighs:
35 (iii) the public interest in protecting the confidentiality of the
36 identity of the journalist's source; and
37 (iv) the public interest in facilitating the exchange of
38 information between journalists and members of the
-

- 1 public so as to facilitate reporting of matters in the
2 public interest; and
3 (d) any previous warrant sought or issued under this Division in
4 relation to the alleged relevant offences referred to in
5 paragraph 27KA(1)(c).
- 6 (3) For the purposes of having regard to the nature and gravity of the
7 conduct constituting the offences referred to in
8 paragraph 27KA(1)(c), the eligible Judge or a nominated AAT
9 member must give weight to the following matters:
- 10 (a) whether that conduct amounts to:
- 11 (i) an activity against the security of the Commonwealth;
12 or
13 (ii) an offence against Chapter 5 of the *Criminal Code*;
- 14 (b) whether that conduct amounts to:
- 15 (i) an activity against the proper administration of
16 Government; or
17 (ii) an offence against Chapter 7 of the *Criminal Code*;
- 18 (c) whether that conduct:
- 19 (i) causes, or has the potential to cause, serious violence, or
20 serious harm, to a person; or
21 (ii) amounts to an offence against Chapter 8 of the *Criminal*
22 *Code*;
- 23 (d) whether that conduct:
- 24 (i) causes, or has the potential to cause, a danger to the
25 community; or
26 (ii) amounts to an offence against Chapter 9 of the *Criminal*
27 *Code*;
- 28 (e) whether that conduct:
- 29 (i) causes, or has the potential to cause, substantial damage
30 to, or loss of, data, property or critical infrastructure; or
31 (ii) amounts to an offence against Chapter 10 of the
32 *Criminal Code*;
- 33 (f) whether that conduct involves, or is related to, the
34 commission of:
- 35 (i) transnational crime; or
36 (ii) serious crime; or
37 (iii) organised crime;
-

that is not covered by any of the preceding paragraphs.

- (4) Subsection (3) does not limit the matters that may be considered by the eligible Judge or nominated AAT member.
- (5) To avoid doubt, this Act does not prevent a data disruption warrant from being issued in a case where the conduct constituting the offences referred to in paragraph 27KA(1)(c) is not covered by subsection (3).
- (6) For the purposes of this section, *secrecy provision* means a provision of a law of the Commonwealth or of a State that prohibits:
 - (a) the communication, divulging or publication of information; or
 - (b) the production of, or the publication of the contents of, a document.

27KD What must a data disruption warrant contain?

- (1) A data disruption warrant must:
 - (a) state that the eligible Judge or nominated AAT member issuing the warrant is satisfied of the matters referred to in subsection 27KC(1) and has had regard to the matters referred to in subsection 27KC(2); and
 - (b) specify:
 - (i) the name of the applicant; and
 - (ii) the alleged relevant offences referred to in paragraph 27KA(1)(c); and
 - (iii) the date the warrant is issued; and
 - (iv) if the target computer is or includes a particular computer—the computer; and
 - (v) if the target computer is or includes a computer on particular premises—the premises; and
 - (vi) if the target computer is or includes a computer associated with, used by or likely to be used by, a known person—the person (whether by name or otherwise); and
 - (vii) the period during which the warrant is in force (see subsection (2)); and

- 1 (viii) the name of the law enforcement officer primarily
2 responsible for executing the warrant; and
3 (ix) any conditions subject to which things may be done
4 under the warrant.
- 5 (2) A warrant may only be issued for a period of no more than 90
6 days.
- 7 Note: The access to, or disruption of, data held in the target computer
8 pursuant to a warrant may be discontinued earlier—see section 27KH.
- 9 (3) In the case of a warrant authorising access to, or disruption of, data
10 held in the target computer on premises that are vehicles, the
11 warrant need only specify the class of vehicle in relation to which
12 the access to, and disruption of, data held in the target computer is
13 authorised.
- 14 (4) A warrant must be signed by the person issuing it and include the
15 person's name.
- 16 (5) As soon as practicable after completing and signing a warrant
17 issued on a remote application, the person issuing it must:
18 (a) inform the applicant of:
19 (i) the terms of the warrant; and
20 (ii) the date on which, and the time at which, the warrant
21 was issued; and
22 (b) give the warrant to the applicant while retaining a copy of the
23 warrant for the person's own record.

24 **27KE What a data disruption warrant authorises**

- 25 (1) A data disruption warrant must authorise the doing of specified
26 things (subject to any restrictions or conditions specified in the
27 warrant) in relation to the relevant target computer.
- 28 (2) The things that may be specified are any of the following that the
29 eligible Judge or nominated AAT member considers appropriate in
30 the circumstances:
31 (a) entering specified premises for the purposes of doing the
32 things mentioned in this subsection;
33 (b) entering any premises for the purposes of gaining entry to, or
34 exiting, the specified premises;

-
- 1 (c) using:
- 2 (i) the target computer; or
- 3 (ii) a telecommunications facility operated or provided by
- 4 the Commonwealth or a carrier; or
- 5 (iii) any other electronic equipment; or
- 6 (iv) a data storage device;
- 7 for the following purposes:
- 8 (v) obtaining access to data (the **relevant data**) that is held
- 9 in the target computer at any time while the warrant is
- 10 in force, in order to determine whether the relevant data
- 11 is covered by the warrant;
- 12 (vi) disrupting the relevant data at any time while the
- 13 warrant is in force, if doing so is likely to assist in
- 14 frustrating the commission of one or more relevant
- 15 offences covered by the warrant;
- 16 (d) if necessary to achieve the purpose mentioned in
- 17 subparagraph (c)(v) or (vi)—adding, copying, deleting or
- 18 altering other data in the target computer;
- 19 (e) if, having regard to other methods (if any) of obtaining
- 20 access to, or disrupting, the relevant data which are likely to
- 21 be as effective, it is reasonable in all the circumstances to do
- 22 so:
- 23 (i) using any other computer or a communication in transit
- 24 to access or disrupt the relevant data; and
- 25 (ii) if necessary to achieve that purpose—adding, copying,
- 26 deleting or altering other data in the computer or the
- 27 communication in transit;
- 28 (f) removing a computer or other thing from premises for the
- 29 purposes of doing any thing specified in the warrant in
- 30 accordance with this subsection, and returning the computer
- 31 or other thing to the premises;
- 32 (g) copying any data to which access has been obtained, and
- 33 that:
- 34 (i) appears to be relevant for the purposes of determining
- 35 whether the relevant data is covered by the warrant; or
- 36 (ii) is covered by the warrant;
- 37 (h) intercepting a communication passing over a
- 38 telecommunications system, if the interception is for the
-

purposes of doing any thing specified in the warrant in accordance with this subsection;

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

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

(3) If:

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

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

the computer or thing must be returned to the premises as soon as is reasonably practicable to do so once the computer or thing is no longer required for the purposes of doing any thing authorised by the warrant.

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

(a) access has been obtained to data; and

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

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

When data is covered by a warrant

(5) For the purposes of this section, data is **covered by** a warrant if disruption of the data is likely to substantially assist as described in paragraph 27KA(1)(c).

When a relevant offence is covered by a warrant

(6) For the purposes of this section, a relevant offence is **covered by** a warrant if the relevant offence is referred to in paragraph 27KA(1)(c).

Certain acts not authorised

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

-
- 1 (a) materially interfere with, interrupt or obstruct:
 - 2 (i) a communication in transit; or
 - 3 (ii) the lawful use by other persons of a computer;
 - 4 unless the addition, deletion or alteration, or the doing of the
 - 5 thing, is necessary to do one or more of the things specified
 - 6 in the warrant; or
 - 7 (b) cause any other material loss or damage to other persons
 - 8 lawfully using a computer, unless the loss or damage is
 - 9 reasonably necessary, and proportionate, to do one or more
 - 10 of the things specified in the warrant.

11 *Warrant must provide for certain matters*

- 12 (8) A data disruption warrant must:
- 13 (a) authorise the use of any force against persons and things that
- 14 is necessary and reasonable to do the things specified in the
- 15 warrant; and
- 16 (b) if the warrant authorises entering premises—state whether
- 17 entry is authorised to be made at any time of the day or night
- 18 or during stated hours of the day or night.

19 *Concealment of access etc.*

- 20 (9) If any thing has been done in relation to a computer under:
- 21 (a) a data disruption warrant; or
- 22 (b) this subsection;
- 23 then, in addition to the things specified in the warrant, the warrant
- 24 authorises the doing of any of the following:
- 25 (c) any thing reasonably necessary to conceal the fact that any
- 26 thing has been done under the warrant or under this
- 27 subsection;
- 28 (d) entering any premises where the computer is reasonably
- 29 believed to be, for the purposes of doing the things
- 30 mentioned in paragraph (c);
- 31 (e) entering any other premises for the purposes of gaining entry
- 32 to or exiting the premises referred to in paragraph (d);
- 33 (f) removing the computer or another thing from any place
- 34 where it is situated for the purposes of doing the things

- 1 mentioned in paragraph (c), and returning the computer or
2 other thing to that place;
- 3 (g) if, having regard to other methods (if any) of doing the things
4 mentioned in paragraph (c) which are likely to be as
5 effective, it is reasonable in all the circumstances to do so:
6 (i) using any other computer or a communication in transit
7 to do those things; and
8 (ii) if necessary to achieve that purpose—adding, copying,
9 deleting or altering other data in the computer or the
10 communication in transit;
- 11 (h) intercepting a communication passing over a
12 telecommunications system, if the interception is for the
13 purposes of doing any thing mentioned in this subsection;
- 14 (i) any other thing reasonably incidental to any of the above;
15 at the following time:
16 (j) at any time while the warrant is in force or within 28 days
17 after it ceases to be in force;
- 18 (k) if none of the things mentioned in paragraph (c) are done
19 within the 28-day period mentioned in paragraph (j)—at the
20 earliest time after that 28-day period at which it is reasonably
21 practicable to do the things mentioned in paragraph (c).
- 22 (10) Subsection (9) does not authorise the doing of a thing that is likely
23 to:
24 (a) materially interfere with, interrupt or obstruct:
25 (i) a communication in transit; or
26 (ii) the lawful use by other persons of a computer;
27 unless the doing of the thing is necessary to do one or more
28 of the things specified in subsection (9); or
29 (b) cause any other material loss or damage to other persons
30 lawfully using a computer, unless the loss or damage is
31 reasonably necessary, and proportionate, to do one or more
32 of the things specified in the warrant or authorised by
33 subsection (9).
- 34 (11) If a computer or another thing is removed from a place in
35 accordance with paragraph (9)(f), the computer or thing must be
36 returned to the place as soon as is reasonably practicable to do so

once the computer or thing is no longer required for the purposes of doing any thing mentioned in paragraph (9)(c).

Statutory conditions

- (12) A data disruption warrant is subject to the following conditions:
- (a) the warrant must not be executed in a manner that results in loss or damage to data unless the damage is reasonably necessary, and proportionate, to do one or more of the things specified in the warrant or authorised by subsection (9);
 - (b) the warrant must not be executed in a manner that causes a person to suffer a permanent loss of:
 - (i) money; or
 - (ii) digital currency; or
 - (iii) property (other than data).
- (13) Subsection (12) does not, by implication, limit the conditions to which a data disruption warrant may be subject.
- (14) The conditions set out in subsection (12) must be specified in a data disruption warrant.

27KF Extension and variation of data disruption warrant

- (1) A law enforcement officer to whom a data disruption warrant has been issued (or another person on the law enforcement officer's behalf) may apply, at any time before the expiry of the warrant:
- (a) for an extension of the warrant for a period of no more than 90 days after the day the warrant would otherwise expire; or
 - (b) for a variation of any of the other terms of the warrant.
- (2) The application is to be made to an eligible Judge or to a nominated AAT member and must be accompanied by the original warrant.
- (3) Sections 27KA and 27KB apply, with any necessary changes, to an application under this section as if it were an application for the warrant.
- (4) The eligible Judge or nominated AAT member may grant an application if satisfied that the matters referred to in

- 1 subsection 27KC(1) still exist, having regard to the matters in
2 subsection 27KC(2).
- 3 (5) If the eligible Judge or nominated AAT member grants the
4 application, the eligible Judge or nominated AAT member must
5 endorse the new expiry date or the other varied term on the original
6 warrant.
- 7 (6) An application may be made under this section more than once.

8 **27KG Revocation of data disruption warrant**

- 9 (1) A data disruption warrant may, by instrument in writing, be
10 revoked by an eligible Judge or nominated AAT member on the
11 initiative of the eligible Judge or nominated AAT member at any
12 time before the expiration of the period of validity specified in the
13 warrant.
- 14 (2) If the circumstances set out in subsection 27KH(2) apply in
15 relation to a data disruption warrant, the chief officer of the law
16 enforcement agency to which the law enforcement officer to whom
17 the warrant was issued belongs or is seconded must, by instrument
18 in writing, revoke the warrant.
- 19 (3) The instrument revoking a warrant must be signed by the eligible
20 Judge, the nominated AAT member or the chief officer of the law
21 enforcement agency, as the case requires.
- 22 (4) If an eligible Judge or nominated AAT member revokes a warrant,
23 the eligible Judge or nominated AAT member must give a copy of
24 the instrument of revocation to the chief officer of the law
25 enforcement agency to which the law enforcement officer to whom
26 the warrant was issued belongs or is seconded.
- 27 (5) If:
28 (a) an eligible Judge or nominated AAT member revokes a
29 warrant; and
30 (b) at the time of the revocation, a law enforcement officer is
31 executing the warrant;
32 the law enforcement officer is not subject to any civil or criminal
33 liability for any act done in the proper execution of that warrant
34 before the officer is made aware of the revocation.

27KH Discontinuance of access and disruption under warrant*Scope*

- (1) This section applies if a data disruption warrant is issued.

Discontinuance of access and disruption

- (2) If:

- (a) the data disruption warrant has been sought by or on behalf of a law enforcement officer; and
- (b) the chief officer of the law enforcement agency to which the law enforcement officer belongs or is seconded is satisfied that access to, and disruption of, data under the warrant is no longer required for the purposes referred to in paragraph 27KA(1)(c);

the chief officer must, in addition to revoking the warrant under section 27KG, take the steps necessary to ensure that access to, and disruption of, data authorised by the warrant is discontinued.

- (3) If the chief officer of a law enforcement agency is notified that a warrant has been revoked by an eligible Judge or a nominated AAT member under section 27KG, the chief officer must take the steps necessary to ensure that access to, and disruption of, data authorised by the warrant is discontinued as soon as practicable.
- (4) If the law enforcement officer to whom the warrant is issued, or who is primarily responsible for executing the warrant, believes that access to, and disruption of, data under the warrant is no longer necessary for the purposes referred to in paragraph 27KA(1)(c), the law enforcement officer must immediately inform the chief officer of the law enforcement agency to which the law enforcement officer belongs or is seconded.

27KJ Relationship of this Division to parliamentary privileges and immunities

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

- (a) each House of the Parliament;

- (b) the members of each House of the Parliament;
(c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

13A Before section 28

Insert:

27KU Sunsetting—emergency authorisation for disruption of data held in a computer

- (1) Subsections 28(1C) and (1D) cease to have effect 5 years after they commence.
- (2) An emergency authorisation for disruption of data held in a computer has no effect after the end of the 5-year period beginning at the commencement of this section.

14 Subsection 28(1B)

After “target computer”, insert “mentioned in subsection (1A)”.

15 After subsection 28(1B)

Insert:

- (1C) A law enforcement officer of the Australian Federal Police or the Australian Crime Commission may apply to an appropriate authorising officer for an emergency authorisation for disruption of data held in a computer (the *target computer*) if, in the course of an investigation of a relevant offence, the law enforcement officer reasonably suspects that:
- (a) an imminent risk of serious violence to a person or substantial damage to property exists; and
 - (b) disruption of data held in the target computer is immediately necessary for the purpose of dealing with that risk; and
 - (ba) there are no alternative methods that:
 - (i) could have been used by law enforcement officers to help reduce or avoid that risk; and
 - (ii) are likely to be as effective as disruption of data held in the target computer; and

-
- 1 (c) the circumstances are so serious and the matter is of such
 2 urgency that disruption of data held in the target computer is
 3 warranted; and
 4 (d) it is not practicable in the circumstances to apply for a data
 5 disruption warrant.
- 6 (1D) The target computer mentioned in subsection (1C) may be any one
 7 or more of the following:
 8 (a) a particular computer;
 9 (b) a computer on particular premises;
 10 (c) a computer associated with, used by or likely to be used by, a
 11 person (whose identity may or may not be known).

12 **16 Subsections 28(3) and (4)**

13 Omit “or (1A)”, substitute “, (1A) or (1C)”.

14 **17 At the end of section 28**

15 Add:

- 16 (4A) In deciding whether to give an emergency authorisation for
 17 disruption of data held in a computer, the appropriate authorising
 18 officer must have regard to:
 19 (a) the extent to which the execution of the emergency
 20 authorisation is likely to result in access to, or disruption of,
 21 data of persons lawfully using a computer; and
 22 (b) whether the likely impact of the execution of the emergency
 23 authorisation on persons lawfully using a computer is
 24 proportionate, having regard to the risk of serious violence or
 25 substantial damage referred to in paragraph (1C)(a).
- 26 (4B) Subsection (4A) does not limit the matters to which the appropriate
 27 authorising officer may have regard.
- 28 *Statutory conditions—disruption of data held in a computer*
- 29 (5) An emergency authorisation for disruption of data held in a
 30 computer is subject to the following conditions:
 31 (a) the authorisation must not be executed in a manner that
 32 results in damage to data unless the damage is reasonably
 33 necessary and proportionate, having regard to the risk of

- 1 serious violence or substantial damage referred to in
2 paragraph (1C)(a);
3 (b) the authorisation must not be executed in a manner that
4 causes a person to suffer a permanent loss of:
5 (i) money; or
6 (ii) digital currency; or
7 (iii) property (other than data).

8 **18 After subsection 32(2A)**

9 Insert:

- 10 (2B) An emergency authorisation for disruption of data held in a
11 computer may authorise anything that a data disruption warrant
12 may authorise.

13 **19 After subsection 32(3A)**

14 Insert:

- 15 (3B) A law enforcement officer may, under an emergency authorisation,
16 disrupt data held in a computer only if the officer is acting in the
17 performance of the officer's duty.

18 **20 Subsection 32(4)**

19 After "(2A)", insert "or (2B)".

20 **21 After subsection 33(2A)**

21 Insert:

- 22 (2B) In the case of an application for an emergency authorisation for
23 disruption of data held in a computer, the application:
24 (a) must specify:
25 (i) the name of the applicant for the approval; and
26 (ii) if a warrant is sought—the nature and duration of the
27 warrant; and
28 (b) must be supported by an affidavit setting out the grounds on
29 which the approval (and warrant, if any) is sought; and
30 (c) must be accompanied by a copy of the written record made
31 under section 31 in relation to the emergency authorisation.

22 After subsection 34(1A)

Insert:

(1B) Before deciding an application for approval of the giving of an emergency authorisation given in response to an application under subsection 28(1C), the eligible Judge or nominated AAT member considering the application must, in particular, and being mindful of the intrusive nature of accessing and disrupting data held in the target computer mentioned in that subsection, consider the following:

- (a) the nature of the risk of serious violence to a person or substantial damage to property;
- (b) the extent to which issuing a data disruption warrant would have helped reduce or avoid the risk;
- (c) the extent to which law enforcement officers could have used alternative methods to help reduce or avoid the risk;
- (d) how much the use of alternative methods could have helped reduce or avoid the risk;
- (e) how much the use of alternative methods would have prejudiced the safety of the person or property because of delay or for another reason;
- (f) whether or not it was practicable in the circumstances to apply for a data disruption warrant.

23 After section 35A

Insert:

35B Judge or nominated AAT member may approve giving of an emergency authorisation for disruption of data held in a computer

(1) After considering an application for approval of the giving of an emergency authorisation in response to an application under subsection 28(1C), the eligible Judge or nominated AAT member may give the approval if satisfied that there were reasonable grounds to suspect that:

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

- 1 (b) disruption of data held in the target computer mentioned in
2 that subsection may have helped reduce the risk; and
3 (c) it was not practicable in the circumstances to apply for a data
4 disruption warrant.
- 5 (2) If, under subsection (1), the eligible Judge or nominated AAT
6 member approves the giving of an emergency authorisation, the
7 eligible Judge or nominated AAT member may:
- 8 (a) unless paragraph (b) applies—issue a data disruption warrant
9 relating to the continued access to, and disruption of, data
10 held in the relevant target computer as if the application for
11 the approval were an application for a data disruption warrant
12 under Division 5 of Part 2; or
- 13 (b) if the eligible Judge or nominated AAT member is satisfied
14 that, since the application for the emergency authorisation,
15 the activity that required access to, and disruption of, data
16 held in the relevant target computer has ceased—order that
17 access to, and disruption of, data held in that computer cease.
- 18 (3) If, under subsection (1), the eligible Judge or nominated AAT
19 member does not approve the giving of an emergency
20 authorisation, the eligible Judge or nominated AAT member may:
- 21 (a) order that access to, and disruption of, data held in the
22 relevant target computer cease; or
- 23 (b) if the eligible Judge or nominated AAT member is of the
24 view that, although the situation did not warrant the
25 emergency authorisation at the time that authorisation was
26 given, the use of a data disruption warrant under Division 5
27 of Part 2 is currently justified—issue a data disruption
28 warrant relating to the subsequent access to, and disruption
29 of, such data as if the application for the approval were an
30 application for a data disruption warrant under Division 5 of
31 Part 2.
- 32 (4) In any case, the eligible Judge or nominated AAT member may
33 order that any information obtained from or relating to the exercise
34 of powers under the emergency authorisation, or any record of that
35 information, be dealt with in a manner specified in the order, so
36 long as the manner does not involve the destruction of that
37 information.
-

24 Section 36

Omit “or 35A”, substitute “, 35A or 35B”.

25 At the end of Part 3

Add:

36A Relationship of this Part to parliamentary privileges and immunities

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

- (a) each House of the Parliament;
- (b) the members of each House of the Parliament;
- (c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

26 Section 41 (paragraph (b) of the definition of *appropriate consenting official*)

Omit “or 43B”, substitute “, 43B, 43C or 43D”.

27 At the end of Part 5

Add:

43C Extraterritorial operation of data disruption warrants

- (1) If, before the issue of a data disruption warrant, it becomes apparent to the applicant for the warrant that there will be a need for access to, and disruption of, data held in a computer:
 - (a) in a foreign country; or
 - (b) on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limits of the territorial sea of Australia;
 the eligible Judge or nominated AAT member considering the application for the warrant must not permit the warrant to authorise that access and disruption unless the eligible Judge or nominated AAT member is satisfied that the access and disruption has been agreed to by an appropriate consenting official of the foreign country.

- 1 (2) If:
- 2 (a) an application is made under section 33 by an appropriate
- 3 authorising officer for approval of the giving of an
- 4 emergency authorisation; and
- 5 (b) the emergency authorisation was given in response to an
- 6 application under subsection 28(1C); and
- 7 (c) before the completion of consideration of that section 33
- 8 application, it becomes apparent to the applicant that there
- 9 will be a need for access to, and disruption of, data held in a
- 10 computer:
- 11 (i) in a foreign country; or
- 12 (ii) on a vessel or aircraft that is registered under the law of
- 13 a foreign country and that is in or above waters beyond
- 14 the outer limits of the territorial sea of Australia;
- 15 the eligible Judge or nominated AAT member to whom the
- 16 section 33 application was made must not permit any data
- 17 disruption warrant issued on consideration of that section 33
- 18 application to authorise that access and disruption unless the
- 19 eligible Judge or nominated AAT member is satisfied that the
- 20 access and disruption has been agreed to by an appropriate
- 21 consenting official of the foreign country.
- 22 (3) If:
- 23 (a) a data disruption warrant has been issued; and
- 24 (b) after the issue of the warrant, it becomes apparent to the law
- 25 enforcement officer primarily responsible for executing the
- 26 warrant that there will be a need for access to, and disruption
- 27 of, data held in a computer that is:
- 28 (i) in a foreign country; or
- 29 (ii) on a vessel or aircraft that is registered under the law of
- 30 a foreign country and that is in or above waters beyond
- 31 the outer limits of the territorial sea of Australia;
- 32 the warrant is taken to permit that access and disruption if, and
- 33 only if, the access and or disruption has been agreed to by an
- 34 appropriate consenting official of the foreign country.
- 35 (4) Subsections (1), (2) and (3) do not apply to a data disruption
- 36 warrant authorising access to, and disruption of, data if:

-
- 1 (a) the person, or each of the persons, responsible for executing
 2 the warrant will be physically present in Australia; and
 3 (b) the location where the data is held is unknown or cannot
 4 reasonably be determined.
- 5 (5) Despite subsections (1), (2) and (3), if:
 6 (a) a vessel that is registered under the law of a foreign country
 7 is in waters beyond the outer limits of the territorial sea of
 8 Australia but not beyond the outer limits of the contiguous
 9 zone of Australia; and
 10 (b) the relevant offences in respect of which it becomes apparent
 11 that access to, and disruption of, data held in a computer on
 12 the vessel will be required are offences relating to the
 13 customs, fiscal, immigration or sanitary laws of Australia;
 14 there is no requirement for the agreement of an appropriate
 15 consenting official of the foreign country concerned in relation to
 16 that access or disruption while the vessel is in such waters.
- 17 (6) Despite subsections (1), (2) and (3), if:
 18 (a) a vessel that is registered under the law of a foreign country
 19 is in waters beyond the outer limits of the territorial sea of
 20 Australia but not beyond the outer limits of the Australian
 21 fishing zone; and
 22 (b) the relevant offences in respect of which it becomes apparent
 23 that access to, and disruption of, data held in a computer on
 24 the vessel will be required are offences against section 100,
 25 100A, 100B, 101, 101A or 101AA of the *Fisheries*
 26 *Management Act 1991* or section 46A, 46B, 46C, 46D, 49A
 27 or 51A of the *Torres Strait Fisheries Act 1984*;
 28 there is no requirement for the agreement of an appropriate
 29 consenting official of the foreign country concerned in relation to
 30 that access or disruption while the vessel is in those waters.
- 31 (7) As soon as practicable after the commencement of access to, and
 32 disruption of, data held in a computer under the authority of a data
 33 disruption warrant in circumstances where consent to that access or
 34 disruption is required:
 35 (a) in a foreign country; or
 36 (b) on a vessel or aircraft that is registered under the law of a
 37 foreign country;
-

1 the chief officer of the law enforcement agency to which the law
2 enforcement officer who applied for the warrant belongs or is
3 seconded must give the Minister evidence in writing that the access
4 and disruption has been agreed to by an appropriate consenting
5 official of the foreign country.

6 (8) An instrument providing evidence of the kind referred to in
7 subsection (7) is not a legislative instrument.

8 (9) If a vessel or aircraft that is registered under the laws of a foreign
9 country is in or above the territorial sea of another foreign country,
10 subsections (1), (2) and (3) have effect as if the reference to an
11 appropriate consenting official of the foreign country were a
12 reference to an appropriate consenting official of each foreign
13 country concerned.

14 (10) For the avoidance of doubt, there is no requirement for the
15 agreement of an appropriate consenting official of the foreign
16 country to the access to, and disruption of, data held in a computer
17 under the authority of a data disruption warrant on a vessel or
18 aircraft of a foreign country that is in Australia or in or above
19 waters within the outer limits of the territorial sea of Australia.

20 **43D Evidence obtained from extraterritorial computer access not to**
21 **be tendered in evidence unless court is satisfied that the**
22 **evidence was properly obtained**

23 Evidence obtained from access to, or disruption of, data held in a
24 computer undertaken in a foreign country in accordance with
25 subsection 43C(1), (2) or (3) in relation to a relevant offence
26 cannot be tendered in evidence to a court in any proceedings
27 relating to the relevant offence unless the court is satisfied that the
28 access or disruption was agreed to by an appropriate consenting
29 official of the foreign country.

30 **28 Subsection 44(1) (after paragraph (aa) of the definition of**
31 **protected information)**

32 Insert:

33 (ab) any information (other than data disruption intercept
34 information) obtained from access to, or disruption of, data
35 under:

- 1 (i) a data disruption warrant; or
- 2 (ii) an emergency authorisation for disruption of data held
- 3 in a computer; or

4 **29 Subsection 44(1) (subparagraph (d)(iv) of the definition of**
5 ***protected information*)**

6 After “obtained”, insert “, purportedly under a computer access warrant
7 or an emergency authorisation for access to data held in a computer,”.

8 **30 Subsection 44(1) (at the end of subparagraph (d)(iv) of the**
9 **definition of *protected information*)**

10 Add “or”.

11 **31 Subsection 44(1) (after subparagraph (d)(iv) of the**
12 **definition of *protected information*)**

13 Insert:

- 14 (v) in a case where the information was obtained,
- 15 purportedly under a data disruption warrant or an
- 16 emergency authorisation for disruption of data held in a
- 17 computer, through access to, or disruption of, data held
- 18 in a computer in a foreign country, or on a vessel or
- 19 aircraft that is registered under the law of a foreign
- 20 country and that is in or above waters beyond the outer
- 21 limit of Australia’s territorial sea—without the
- 22 agreement of the appropriate consenting official of that
- 23 foreign country, and of any other foreign country,
- 24 whose agreement is required under section 43C;

25 **32 Subsection 44(1) (paragraph (d) of the definition of**
26 ***protected information*)**

27 Omit “such”.

28 **33 Subsection 44(1) (note to the definition of *protected***
29 ***information*)**

30 Omit “Note”, substitute “Note 1”.

34 Subsection 44(1) (at the end of the definition of *protected information*)

Add:

Note 2: For protection of data disruption intercept information, see Part 2-6 of the *Telecommunications (Interception and Access) Act 1979*.

35 After subsection 45(6)

Insert:

(6A) Protected information may be communicated by an Ombudsman official to an IGIS official for the purposes of the IGIS official exercising powers, or performing functions or duties, as an IGIS official.

36 Paragraph 46(1)(a)

Omit “or general computer access intercept information”, substitute “, general computer access intercept information or data disruption intercept information”.

37 At the end of paragraph 46(2)(ab)

Add “or”.

38 After paragraph 46(2)(ab)

Insert:

(ac) disrupting data held in a computer;

39 After section 47A

Insert:

47B Protection of data disruption technologies and methods

(1) In a proceeding, a person may object to the disclosure of information on the ground that the information, if disclosed, could reasonably be expected to reveal details of data disruption technologies or methods.

(2) If the person conducting or presiding over the proceeding is satisfied that the ground of objection is made out, the person may

order that the person who has the information not be required to disclose it in the proceeding.

- (3) In determining whether or not to make an order under subsection (2), the person conducting or presiding over the proceeding must take into account whether disclosure of the information:
- (a) is necessary for the fair trial of the defendant; or
 - (b) is in the public interest.
- (4) Subsection (2) does not affect a provision of another law under which a law enforcement officer cannot be compelled to disclose information or make statements in relation to the information.
- (5) If the person conducting or presiding over a proceeding is satisfied that publication of any information disclosed in the proceeding could reasonably be expected to reveal details of data disruption technologies or methods, the person must make any orders prohibiting or restricting publication of the information that the person considers necessary to ensure that those details are not revealed.
- (6) Subsection (5) does not apply to the extent that the person conducting or presiding over the proceeding considers that the interests of justice require otherwise.

- (7) In this section:

data disruption technologies or methods means technologies or methods relating to the use of:

- (a) a computer; or
- (b) a telecommunications facility operated or provided by the Commonwealth or a carrier; or
- (c) any other electronic equipment; or
- (d) a data storage device;

for either or both of the following purposes:

- (e) disrupting data held in the computer;
 - (f) obtaining access to data held in the computer;
- where the technologies or methods have been, or are being, deployed in giving effect to:
- (g) a data disruption warrant; or

- 1 (h) an emergency authorisation for disruption of data held in a
2 computer.

3 *proceeding* includes a proceeding before a court, tribunal or Royal
4 Commission.

5 **40 After subsection 49(2C)**

6 Insert:

7 (2D) In the case of:

- 8 (a) a data disruption warrant for disruption of data held in a
9 computer; or
10 (b) an emergency authorisation for disruption of data held in a
11 computer;

12 the report must:

- 13 (c) state whether the warrant or authorisation was executed; and
14 (d) if so:
15 (i) state the name of the person primarily responsible for
16 the execution of the warrant or authorisation; and
17 (ii) state the name of each person involved in accessing or
18 disrupting data under the warrant or authorisation; and
19 (iii) state the period during which the data was accessed or
20 disrupted; and
21 (iv) state the name, if known, of any person whose data was
22 accessed or disrupted; and
23 (v) give details of any premises at which the computer was
24 located; and
25 (vi) give details of the benefit of the use of the warrant or
26 authorisation in frustrating criminal activity; and
27 (vii) give details of the access to, and disruption of, data
28 under the warrant or authorisation; and
29 (viii) give details of the compliance with the conditions (if
30 any) to which the warrant or authorisation was subject;
31 and
32 (e) if the warrant or authorisation was extended or varied, state:
33 (i) the number of extensions or variations; and
34 (ii) the reasons for them.

41 After section 49B

Insert:

49C Notification to Ombudsman of things done under a data disruption warrant

(1) If:

- (a) a data disruption warrant was issued in response to an application made by a law enforcement officer of a law enforcement agency; and
- (b) a thing mentioned in subsection 27KE(2) was done under the warrant;

the chief officer of the law enforcement agency must:

- (c) notify the Ombudsman:
 - (i) that the warrant was issued; and
 - (ii) of the fact that the thing was done under the warrant; and
- (d) do so within 7 days after the thing was done.

(2) If:

- (a) a data disruption warrant was issued in response to an application made by a law enforcement officer of a law enforcement agency; and
- (b) the person executing the warrant becomes aware that a thing mentioned in subsection 27KE(2) that was done under the warrant has caused material loss or damage to one or more persons lawfully using a computer;

the chief officer of the law enforcement agency must:

- (c) notify the Ombudsman:
 - (i) that the thing has caused material loss or damage to one or more persons lawfully using a computer; and
 - (ii) of the particulars of that loss or damage; and
- (d) do so within 7 days after the person executing the warrant became so aware.

42 After paragraph 50(1)(ea)

Insert:

- (eb) if the agency is the Australian Federal Police or the Australian Crime Commission—the kinds of offences targeted by data disruption warrants issued during that year in response to applications made by or on behalf of law enforcement officers of the agency; and

43 Paragraph 51(b)

Omit “or 27G(4)”, substitute “, 27G(4) or 27KG(4)”.

44 At the end of subsection 62(1)

Add:

; or (d) anything done by the law enforcement officer in connection with:

- (i) the communication by a person to another person of; or
 - (ii) the making use of; or
 - (iii) the making of a record of; or
 - (iv) the custody of a record of;
- information obtained from access to, or disruption of, data under:
- (v) a data disruption warrant; or
 - (vi) an emergency authorisation for disruption of data held in a computer.

45 Subsection 62(3)

Omit “or 35A”, substitute “, 35A or 35B”.

46 Paragraph 64(2)(a)

After “access to”, insert “, or disrupting,”.

46A At the end of section 64

Add:

(3) If:

- (a) a person suffers loss or injury as a result of the use of:
 - (i) a computer; or
 - (ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or
 - (iii) any other electronic equipment; or

-
- 1 (iv) a data storage device;
 - 2 for the purpose of obtaining access to, or disrupting, data that
 - 3 is held in the computer; and
 - 4 (b) the use of the computer, facility, equipment or device, as the
 - 5 case may be, was authorised by an emergency authorisation
 - 6 for disruption of data held in a computer; and
 - 7 (c) the giving of the emergency authorisation was not approved
 - 8 under section 35B;
 - 9 the Commonwealth is liable to pay to the person who has suffered
 - 10 the loss or injury:
 - 11 (d) such compensation as is agreed on between the
 - 12 Commonwealth and that person; or
 - 13 (e) in default of such an agreement—such compensation as is
 - 14 determined by action against the Commonwealth in a court
 - 15 of a State or Territory that has jurisdiction in relation to the
 - 16 matter.

17 **47 After section 64A**

18 Insert:

19 **64B Person with knowledge of a computer or a computer system to** 20 **assist disruption of data etc.**

- 21 (1) A law enforcement officer of the Australian Federal Police or the
- 22 Australian Crime Commission (or another person on the officer's
- 23 behalf) may apply to an eligible Judge or to a nominated AAT
- 24 member for an order (the *assistance order*) requiring a specified
- 25 person to provide any information or assistance that is reasonable
- 26 and necessary to allow the law enforcement officer to do one or
- 27 more of the following:
- 28 (a) disrupt data held in a computer that is the subject of:
- 29 (i) a data disruption warrant; or
- 30 (ii) an emergency authorisation given in response to an
- 31 application under subsection 28(1C);
- 32 (b) access data that is held in the computer described in
- 33 paragraph (a);
- 34 (c) copy data held in the computer described in paragraph (a) to
- 35 a data storage device;

1 (d) convert into documentary form or another form intelligible to
2 a law enforcement officer:

- 3 (i) data held in the computer described in paragraph (a); or
4 (ii) data held in a data storage device to which the data was
5 copied as described in paragraph (c).

6 *Grant of assistance order*

7 (2) The eligible Judge or nominated AAT member may grant the
8 assistance order if the eligible Judge or nominated AAT member is
9 satisfied that:

10 (a) in a case where the computer is the subject of a data
11 disruption warrant—disruption of data held in the computer
12 is:

- 13 (i) likely to substantially assist in frustrating the
14 commission of the offences that are covered by the
15 warrant (within the meaning of section 27KE); and
16 (ii) justifiable and proportionate, having regard to those
17 offences; and

18 (aa) in a case where the computer is the subject of a data
19 disruption warrant—the assistance order is reasonable and
20 necessary to enable the warrant to be executed; and

21 (ab) in a case where the computer is the subject of a data
22 disruption warrant—the assistance order is justifiable and
23 proportionate, having regard to:

- 24 (i) the nature and gravity of the conduct constituting the
25 offences referred to in paragraph 27KA(1)(c); and
26 (ii) the likely impact of compliance with the assistance
27 order on the specified person, so far as that matter is
28 known to the eligible Judge or nominated AAT
29 member; and
30 (iii) the likely impact of compliance with the assistance
31 order on other persons (including persons who may
32 lawfully be using the computer), so far as that matter is
33 known to the eligible Judge or nominated AAT
34 member; and

35 (b) in a case where the computer is the subject of an emergency
36 authorisation given in response to an application under
37 subsection 28(1C):

-
- 1 (i) there is an imminent risk of serious violence to a person
 2 or substantial damage to property; and
 3 (ii) disruption of data held in the computer is immediately
 4 necessary for the purpose of dealing with the risk; and
 5 (ba) in a case where the computer is the subject of an emergency
 6 authorisation given in response to an application under
 7 subsection 28(1C)—the assistance order is reasonable and
 8 necessary to enable the emergency authorisation to be
 9 executed; and
 10 (bb) in a case where the computer is the subject of an emergency
 11 authorisation given in response to an application under
 12 subsection 28(1C)—the assistance order is justifiable and
 13 proportionate, having regard to:
 14 (i) the risk of serious violence or substantial damage
 15 referred to in paragraph 28(1C)(a); and
 16 (ii) the likely impact of compliance with the assistance
 17 order on the specified person, so far as that matter is
 18 known to the eligible Judge or nominated AAT
 19 member; and
 20 (iii) the likely impact of compliance with the assistance
 21 order on other persons (including persons who may
 22 lawfully be using the computer), so far as that matter is
 23 known to the eligible Judge or nominated AAT
 24 member; and
 25 (c) in a case where:
 26 (i) the computer is the subject of a data disruption warrant;
 27 and
 28 (ii) the assistance order requires the specified person to
 29 provide information or assistance to allow the law
 30 enforcement officer to do a thing referred to in
 31 paragraph (1)(b), (c) or (d) in relation to data;
 32 doing the thing is for the purpose of determining whether the
 33 data is covered by the warrant (within the meaning of
 34 section 27KE); and
 35 (d) in a case where:
 36 (i) the computer is the subject of an emergency
 37 authorisation given in response to an application under
 38 subsection 28(1C); and
-

- 1 (ii) the assistance order requires the specified person to
2 provide information or assistance to allow the law
3 enforcement officer to do a thing referred to in
4 paragraph (1)(b), (c) or (d) in relation to data;
5 doing the thing is for the purpose of determining whether
6 disruption of the data is immediately necessary for the
7 purpose of dealing with an imminent risk of serious violence
8 to a person or substantial damage to property; and
9 (e) the specified person is:
10 (i) in a case where the computer is the subject of a data
11 disruption warrant—reasonably suspected of having
12 committed any of the relevant offences referred to in
13 paragraph 27KA(1)(c); or
14 (ii) in a case where the computer is the subject of
15 emergency authorisation—reasonably suspected of
16 having committed the relevant offence referred to in
17 subsection 28(1C); or
18 (iii) the owner or lessee of the computer; or
19 (iv) an employee of the owner or lessee of the computer; or
20 (v) a person engaged under a contract for services by the
21 owner or lessee of the computer; or
22 (vi) a person who uses or has used the computer; or
23 (vii) a person who is or was a system administrator for the
24 system including the computer; and
25 (f) the specified person has relevant knowledge of:
26 (i) the computer or a computer network of which the
27 computer forms or formed a part; or
28 (ii) measures applied to protect data held in the computer.
29 (2A) In determining whether the assistance order should be granted, the
30 eligible Judge or nominated AAT member must have regard to
31 whether the specified person is, or has been, subject to:
32 (a) another order under this section; or
33 (b) an order under section 64A of this Act; or
34 (c) an order under section 3LA or 3ZZVG of the *Crimes Act*
35 *1914*;
36 so far as that matter is known to the eligible Judge or nominated
37 AAT member.
-

1 (2B) Subsection (2A) does not limit the matters to which the eligible
2 Judge or nominated AAT member may have regard.

3 *Duration of assistance order*

4 (2C) If an assistance order is granted in relation to a computer that is the
5 subject of a data disruption warrant, the order ceases to be in force
6 when the warrant ceases to be in force.

7 (2D) If an assistance order is granted in relation to a computer that is the
8 subject of an emergency authorisation given in response to an
9 application under subsection 28(1C), the order ceases to be in force
10 when the emergency authorisation ceases to be in force.

11 *Protection from civil liability*

12 (2E) A person is not subject to any civil liability in respect of an act
13 done by the person:

- 14 (a) in compliance with an assistance order; or
- 15 (b) in good faith in purported compliance with an assistance
16 order.

17 *Offence*

- 18 (3) A person commits an offence if:
 - 19 (a) the person is subject to an order under this section; and
 - 20 (b) the person is capable of complying with a requirement in the
21 order; and
 - 22 (c) the person omits to do an act; and
 - 23 (d) the omission contravenes the requirement.

24 Penalty for contravention of this subsection: Imprisonment for 10
25 years or 600 penalty units, or both.

26 **48 Paragraph 65(1A)(a)**

27 After “computer access warrant”, insert “, data disruption warrant”.

28 **49 After subsection 65(1A)**

29 Insert:

30 (1B) If:

- 1 (a) data is disrupted purportedly under:
2 (i) a data disruption warrant; or
3 (ii) an emergency authorisation for disruption of data held
4 in a computer; and
5 (b) there is a defect or irregularity in relation to the warrant or
6 emergency authorisation; and
7 (c) but for that defect or irregularity, the warrant or emergency
8 authorisation would be a sufficient authority for disrupting
9 the data;
10 disruption of the data is taken to be as valid as if the warrant or
11 emergency authorisation did not have that defect or irregularity.

12 **50 Subsection 65(2)**

13 Omit “or (1A)”, substitute “, (1A) or (1B)”.

14 **51 After section 65B**

15 Insert:

16 **65C Evidence obtained from access to, or disruption of, data under**
17 **a data disruption warrant etc.**

18 This Act does not prevent evidence obtained from access to, or
19 disruption of, data under:
20 (a) a data disruption warrant; or
21 (b) an emergency authorisation for disruption of data held in a
22 computer;
23 from being admissible as evidence in a proceeding relating to a
24 relevant offence.

25 ***Telecommunications (Interception and Access) Act 1979***

26 **52 Subsection 5(1)**

27 Insert:

28 ***data disruption intercept information*** means information obtained
29 under a data disruption warrant by intercepting a communication
30 passing over a telecommunications system.

data disruption warrant has the same meaning as in the
Surveillance Devices Act 2004.

53 Subsection 5(1) (at the end of the definition of *restricted record*)

Add “or a record of data disruption intercept information”.

54 Subsection 5(1) (paragraph (b) of the definition of *warrant*)

After “general computer access warrant”, insert “, a data disruption warrant”.

55 Paragraph 7(2)(bb)

After “27E(7)”, insert “or 27KE(9)”.

56 After section 63AC

Insert:

63AD Dealing in data disruption intercept information etc.

- (1) A person may, for the purposes of doing a thing authorised by a data disruption warrant:
 - (a) communicate data disruption intercept information to another person; or
 - (b) make use of data disruption intercept information; or
 - (c) make a record of data disruption intercept information; or
 - (d) give data disruption intercept information in evidence in a proceeding.
- (2) A person may:
 - (a) communicate data disruption intercept information to another person; or
 - (b) make use of data disruption intercept information; or
 - (c) make a record of data disruption intercept information;if the information relates, or appears to relate, to the involvement, or likely involvement, of a person in one or more of the following activities:
 - (d) activities that present a significant risk to a person’s safety;

- 1 (e) acting for, or on behalf of, a foreign power (within the
2 meaning of the *Australian Security Intelligence Organisation*
3 *Act 1979*);
- 4 (f) activities that are, or are likely to be, a threat to security;
- 5 (g) activities that pose a risk, or are likely to pose a risk, to the
6 operational security (within the meaning of the *Intelligence*
7 *Services Act 2001*) of ASIS (within the meaning of that Act);
- 8 (h) activities that pose a risk, or are likely to pose a risk, to the
9 operational security (within the ordinary meaning of that
10 expression) of the Organisation or of AGO or ASD (within
11 the meanings of the *Intelligence Services Act 2001*);
- 12 (i) activities related to the proliferation of weapons of mass
13 destruction or the movement of goods listed from time to
14 time in the Defence and Strategic Goods List (within the
15 meaning of regulation 13E of the *Customs (Prohibited*
16 *Exports) Regulations 1958*);
- 17 (j) activities related to a contravention, or an alleged
18 contravention, by a person of a UN sanction enforcement law
19 (within the meaning of the *Charter of the United Nations Act*
20 *1945*).
- 21 (3) A person may, in connection with:
- 22 (a) the performance by an Ombudsman official of the
23 Ombudsman official's functions or duties; or
- 24 (b) the exercise by an Ombudsman official of the Ombudsman
25 official's powers;
- 26 communicate to the Ombudsman official, or make use of, or make
27 a record of, data disruption intercept information.
- 28 (4) An Ombudsman official may, in connection with:
- 29 (a) the performance by the Ombudsman official of the
30 Ombudsman official's functions or duties; or
- 31 (b) the exercise by the Ombudsman official of the Ombudsman
32 official's powers;
- 33 communicate to another person, or make use of, or make a record
34 of, data disruption intercept information.
- 35 (5) A person may, in connection with:
- 36 (a) the performance by an IGIS official of the IGIS official's
37 functions or duties; or
-

-
- 1 (b) the exercise by an IGIS official of the IGIS official's powers;
 2 communicate to the IGIS official, or make use of, or make a record
 3 of, data disruption intercept information.
- 4 (6) An IGIS official may, in connection with:
 5 (a) the performance by the IGIS official of the IGIS official's
 6 functions or duties; or
 7 (b) the exercise by the IGIS official of the IGIS official's
 8 powers;
 9 communicate to another person, or make use of, or make a record
 10 of, data disruption intercept information.
- 11 (7) If:
 12 (a) information was obtained by intercepting a communication
 13 passing over a telecommunications system; and
 14 (b) the interception was purportedly for the purposes of doing a
 15 thing specified in a data disruption warrant; and
 16 (c) the interception was not authorised by the data disruption
 17 warrant;
 18 then:
 19 (d) a person may, in connection with:
 20 (i) the performance by an Ombudsman official of the
 21 Ombudsman official's functions or duties; or
 22 (ii) the exercise by an Ombudsman official of the
 23 Ombudsman official's powers;
 24 communicate to the Ombudsman official, or make use of, or
 25 make a record of, that information; and
 26 (e) an Ombudsman official may, in connection with:
 27 (i) the performance by the Ombudsman official of the
 28 Ombudsman official's functions or duties; or
 29 (ii) the exercise by the Ombudsman official of the
 30 Ombudsman official's powers;
 31 communicate to another person, or make use of, or make a
 32 record of, that information; and
 33 (f) a person may, in connection with:
 34 (i) the performance by an IGIS official of the IGIS
 35 official's functions or duties; or

- 1 (ii) the exercise by an IGIS official of the IGIS official's
2 powers;
3 communicate to the IGIS official, or make use of, or make a
4 record of, that information; and
5 (g) an IGIS official may, in connection with:
6 (i) the performance by the IGIS official of the IGIS
7 official's functions or duties; or
8 (ii) the exercise by the IGIS official of the IGIS official's
9 powers;
10 communicate to another person, or make use of, or make a
11 record of, that information.
- 12 (8) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution
13 for an offence against section 63 of this Act, an Ombudsman
14 official or an IGIS official does not bear an evidential burden in
15 relation to the matters in subsection (4), (6) or (7) of this section.

16 **57 Paragraph 67(1)(a)**

17 Omit "or general computer access intercept information", substitute "
18 general computer access intercept information or data disruption
19 intercept information".

20 **58 Section 68**

21 After "general computer access intercept information", insert "or data
22 disruption intercept information".

23 **59 Subsection 74(1)**

24 After "general computer access intercept information", insert ", data
25 disruption intercept information".

26 **60 Subsection 75(1)**

27 After "general computer access warrant", insert ", a data disruption
28 warrant".

29 **61 Paragraphs 77(1)(a) and (b)**

30 After "63AC,", insert "63AD,".

31 **62 After paragraph 108(2)(cb)**

32 Insert:

-
- 1 (cc) accessing a stored communication under a data disruption
2 warrant; or

Schedule 2—Network activity warrants

Part 1—Main amendments

Surveillance Devices Act 2004

1 After paragraph 3(aab)

Insert:

- (aac) to establish procedures for the chief officer of the Australian Federal Police or the Australian Crime Commission to obtain warrants that:
 - (i) authorise access to data held in computers; and
 - (ii) will substantially assist in the collection of intelligence that relates to criminal networks of individuals; and

2 After subsection 4(4B)

Insert:

- (4C) For the avoidance of doubt, it is intended that a warrant may be issued under this Act:
 - (a) for access to data held in a computer; and
 - (b) in relation to the collection of intelligence that relates to a criminal network of individuals.

3 Subsection 6(1)

Insert:

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

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

- (a) use the same electronic service as at least one other individual in the group;
- (b) communicate with at least one other individual in the group by electronic communication.

electronic communication means a communication of information:

- (a) whether in the form of text; or
(b) whether in the form of data; or
(c) whether in the form of speech, music or other sounds; or
(d) whether in the form of visual images (animated or otherwise); or
(e) whether in any other form; or
(f) whether in any combination of forms;
by means of guided and/or unguided electromagnetic energy.

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

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

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

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

4 Subsection 6(1) (definition of *remote application*)

Omit “or 27KB”, substitute, “, 27KB or 27KL”.

5 Subsection 6(1) (definition of *unsworn application*)

Omit “or 27KA(4) and (5)”, substitute “, 27KA(4) and (5) or 27KK(5) and (6)”.

6 Subsection 6(1) (at the end of the definition of *warrant*)

Add:
; or (e) a network activity warrant.

7 At the end of subsection 10(1)

Add:
; (e) a network activity warrant.

8 After section 7

Insert:

7A Criminal network of individuals

- (1) For the purposes of this Act, a *criminal network of individuals* is an electronically linked group of individuals, where:
- (a) in a case where each individual in the group uses, or is likely to use, the same electronic service as at least one other individual in the group—the use of that electronic service enables any of the individuals in the group to:
 - (i) engage in conduct that constitutes a relevant offence; or
 - (ii) communicate with any of the individuals in the group about any of the individuals in the group engaging in conduct that constitutes a relevant offence; or
 - (iii) facilitate the engagement, by another person (whether or not an individual in the group), in conduct that constitutes a relevant offence; or
 - (iv) communicate with any of the individuals in the group about facilitating the engagement, by another person (whether or not an individual in the group), in conduct that constitutes a relevant offence; or
 - (b) in a case where each individual in the group communicates with at least one other individual in the group by electronic communication—the electronic communication enables any of the individuals in the group to:
 - (i) engage in conduct that constitutes a relevant offence; or
 - (ii) communicate with any of the individuals in the group about any of the individuals in the group engaging in conduct that constitutes a relevant offence; or
 - (iii) facilitate the engagement, by another person (whether or not an individual in the group), in conduct that constitutes a relevant offence; or
 - (iv) communicate with any of the individuals in the group about facilitating the engagement, by another person (whether or not an individual in the group), in conduct that constitutes a relevant offence.
- (2) For the purposes of subsection (1), it is immaterial whether:
- (a) the identities of the individuals in the group can be ascertained; or
 - (b) the details of the relevant offences can be ascertained; or

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

3 **9 At the end of Part 2**

4 Add:

5 **Division 6—Network activity warrants**

6 **27KKA Sunsetting**

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

8 **27KK Application for network activity warrant**

- 9 (1) The chief officer of the Australian Federal Police or the Australian
10 Crime Commission may apply for the issue of a network activity
11 warrant if the chief officer suspects on reasonable grounds that:
12 (a) a group of individuals is a criminal network of individuals;
13 and
14 (b) access to data held in a computer (the *target computer*) that
15 is, from time to time, used, or likely to be used, by any of the
16 individuals in the group will substantially assist in the
17 collection of intelligence that:
18 (i) relates to the group or to any of the individuals in the
19 group; and
20 (ii) is relevant to the prevention, detection or frustration of
21 one or more kinds of relevant offences.
- 22 (2) For the purposes of subsection (1), it is immaterial whether:
23 (a) the identities of the individuals in the group can be
24 ascertained; or
25 (b) the target computer can be identified; or
26 (c) the location of the target computer can be identified; or
27 (d) there are likely to be changes, from time to time, in the
28 composition of the group.

29 *Procedure for making applications*

- 30 (3) An application under subsection (1) may be made to an eligible
31 Judge or to a nominated AAT member.

- 1 (4) An application:
2 (a) must specify:
3 (i) the name of the applicant; and
4 (ii) the nature and duration of the warrant sought; and
5 (b) subject to this section, must be supported by an affidavit
6 setting out the grounds on which the warrant is sought.

7 *Unsworn applications*

- 8 (5) If the chief officer of the Australian Federal Police or the
9 Australian Crime Commission believes that:
10 (a) immediate access to data held in the target computer referred
11 to in subsection (1) will substantially assist as described in
12 paragraph (1)(b); and
13 (b) it is impracticable for an affidavit to be prepared or sworn
14 before an application for a warrant is made by the chief
15 officer;
16 an application by the chief officer for a warrant under
17 subsection (1) may be made before an affidavit is prepared or
18 sworn.
- 19 (6) If subsection (5) applies, the applicant must:
20 (a) provide as much information as the eligible Judge or
21 nominated AAT member considers is reasonably practicable
22 in the circumstances; and
23 (b) not later than 72 hours after the making of the application,
24 send a duly sworn affidavit to the eligible Judge or
25 nominated AAT member, whether or not a warrant has been
26 issued.

27 *Target computer*

- 28 (7) The target computer referred to in subsection (1):
29 (a) must be a computer that is, from time to time, used or likely
30 to be used by an individual (whose identity may or may not
31 be known); and
32 (b) may be one or more of the following:
33 (i) a particular computer;
34 (ii) a computer that is, from time to time, on particular
35 premises.

27KL Remote application

- (1) If the chief officer of the Australian Federal Police or the Australian Crime Commission believes that it is impracticable for an application for a network activity warrant to be made in person, the application may be made under section 27KK by telephone, fax, email or any other means of communication.
- (2) If transmission by fax is available and an affidavit has been prepared, the person applying must transmit a copy of the affidavit, whether sworn or unsworn, to the eligible Judge or to the nominated AAT member who is to determine the application.

27KM Determining the application

- (1) An eligible Judge or a nominated AAT member may issue a network activity warrant if satisfied:
- (a) that there are reasonable grounds for the suspicion founding the application for the warrant; and
 - (aa) that the issue of the warrant is justified and proportionate, having regard to the kinds of offences in relation to which information will be obtained under the warrant; and
 - (b) in the case of an unsworn application—that it would have been impracticable for an affidavit to have been sworn or prepared before the application was made; and
 - (c) in the case of a remote application—that it would have been impracticable for the application to have been made in person.
- (2) In determining whether a network activity warrant should be issued, the eligible Judge or nominated AAT member must have regard to:
- (a) the nature and gravity of the conduct constituting the kinds of offences in relation to which information will be obtained under the warrant; and
 - (b) the extent to which access to data under the warrant will assist in the collection of intelligence that:
 - (i) relates to the group referred to in paragraph 27KK(1)(a) or to any of the individuals in the group; and

- 1 (ii) is relevant to the prevention, detection or frustration of
2 one or more kinds of relevant offences; and
3 (c) the likely intelligence value of any information sought to be
4 obtained; and
5 (d) whether the things authorised by the warrant are
6 proportionate to the likely intelligence value of any
7 information sought to be obtained; and
8 (e) the existence of any alternative, or less intrusive, means of
9 obtaining the information sought to be obtained; and
10 (f) the extent to which the execution of the warrant is likely to
11 result in access to data of persons who are lawfully using a
12 computer, and any privacy implications (to the extent known
13 to the eligible Judge or nominated AAT member) resulting
14 from that access; and
15 (fa) if:
16 (i) the eligible Judge or nominated AAT member believes
17 on reasonable grounds that the data covered by the
18 warrant (within the meaning of section 27KP) is data of
19 a person who is working in a professional capacity as a
20 journalist or of an employer of such a person; and
21 (ii) each of the offences referred to in
22 paragraph 27KK(1)(b) is an offence against a secrecy
23 provision;
24 whether the public interest in issuing the warrant outweighs:
25 (iii) the public interest in protecting the confidentiality of the
26 identity of the journalist's source; and
27 (iv) the public interest in facilitating the exchange of
28 information between journalists and members of the
29 public so as to facilitate reporting of matters in the
30 public interest; and
31 (g) any previous warrant sought or issued under this Division in
32 relation to the group referred to in paragraph 27KK(1)(a).
33 (2A) For the purposes of having regard to the nature and gravity of the
34 conduct constituting the kinds of offences in relation to which
35 information will be obtained under the warrant, the eligible Judge
36 or nominated AAT member must give weight to the following
37 matters:
38 (a) whether that conduct amounts to:
-

- 1 (i) an activity against the security of the Commonwealth;
2 or
3 (ii) an offence against Chapter 5 of the *Criminal Code*;
4 (b) whether that conduct amounts to:
5 (i) an activity against the proper administration of
6 Government; or
7 (ii) an offence against Chapter 7 of the *Criminal Code*;
8 (c) whether that conduct:
9 (i) causes, or has the potential to cause, serious violence, or
10 serious harm, to a person; or
11 (ii) amounts to an offence against Chapter 8 of the *Criminal*
12 *Code*;
13 (d) whether that conduct:
14 (i) causes, or has the potential to cause, a danger to the
15 community; or
16 (ii) amounts to an offence against Chapter 9 of the *Criminal*
17 *Code*;
18 (e) whether that conduct:
19 (i) causes, or has the potential to cause, substantial damage
20 to, or loss of, data, property or critical infrastructure; or
21 (ii) amounts to an offence against Chapter 10 of the
22 *Criminal Code*;
23 (f) whether that conduct involves, or is related to, the
24 commission of:
25 (i) transnational crime; or
26 (ii) serious crime; or
27 (iii) organised crime;
28 that is not covered by any of the preceding paragraphs.
29 (2B) Subsection (2A) does not limit the matters that may be considered
30 by the eligible Judge or nominated AAT member.
31 (2C) To avoid doubt, this Act does not prevent a network activity
32 warrant from being issued in a case where the conduct constituting
33 the kinds of offences in relation to which information will be
34 obtained under the warrant is not covered by subsection (2A).

- 1 (3) If a network activity warrant is issued in response to an application
2 made by the chief officer of the Australian Federal Police or the
3 Australian Crime Commission, the chief officer must:
4 (a) notify the issue of the warrant to the Inspector-General of
5 Intelligence and Security; and
6 (b) do so within 7 days after the issue of the warrant.
- 7 (4) For the purposes of this section, *secrecy provision* means a
8 provision of a law of the Commonwealth or of a State that
9 prohibits:
10 (a) the communication, divulging or publication of information;
11 or
12 (b) the production of, or the publication of the contents of, a
13 document.

14 **27KN What must a network activity warrant contain?**

- 15 (1) A network activity warrant must:
16 (a) state that the eligible Judge or nominated AAT member
17 issuing the warrant is satisfied of the matters referred to in
18 subsection 27KM(1) and has had regard to the matters
19 referred to in subsection 27KM(2); and
20 (b) specify:
21 (i) the name of the applicant; and
22 (ii) the kinds of relevant offences in respect of which the
23 warrant is issued; and
24 (iii) the criminal network of individuals to which the warrant
25 relates; and
26 (iv) the date the warrant is issued; and
27 (v) the period during which the warrant is in force (see
28 subsection (2)); and
29 (vi) the name of the law enforcement officer primarily
30 responsible for executing the warrant; and
31 (vii) any conditions subject to which things may be done
32 under the warrant; and
33 (c) if the warrant authorises the use of a surveillance device—
34 specify:
35 (i) the surveillance device authorised to be used; and

- 1 (ii) the purpose or purposes for which the surveillance
2 device may be used under the warrant.
- 3 (2) A warrant may only be issued for a period of no more than 90
4 days.
- 5 Note: The access to data held in the target computer pursuant to a warrant
6 may be discontinued earlier—see section 27KS.
- 7 (3) A warrant must be signed by the person issuing it and include the
8 person's name.
- 9 (4) For the purposes of subparagraph (1)(b)(iii), a criminal network of
10 individuals may be specified by identifying one or more matters or
11 things that are sufficient to identify the criminal network of
12 individuals.
- 13 (5) As soon as practicable after completing and signing a warrant
14 issued on a remote application, the person issuing it must:
- 15 (a) inform the applicant of:
- 16 (i) the terms of the warrant; and
17 (ii) the date on which, and the time at which, the warrant
18 was issued; and
- 19 (b) give the warrant to the applicant while retaining a copy of the
20 warrant for the person's own record.

21 **27KP What a network activity warrant authorises**

- 22 (1) A network activity warrant must authorise the doing of specified
23 things (subject to any restrictions or conditions specified in the
24 warrant) in relation to the relevant target computer.
- 25 (2) The things that may be specified are any of the following that the
26 eligible Judge or nominated AAT member considers appropriate in
27 the circumstances:
- 28 (a) entering specified premises for the purposes of doing the
29 things mentioned in this subsection;
- 30 (b) entering any premises for the purposes of gaining entry to, or
31 exiting, the specified premises;
- 32 (c) using:
- 33 (i) the target computer; or

- 1 (ii) a telecommunications facility operated or provided by
2 the Commonwealth or a carrier; or
3 (iii) any other electronic equipment; or
4 (iv) a data storage device;
5 for the purpose of obtaining access to data (the *relevant data*)
6 that is held in the target computer at any time while the
7 warrant is in force, in order to determine whether the relevant
8 data is covered by the warrant;
9 (d) if necessary to achieve the purpose mentioned in
10 paragraph (c)—adding, copying, deleting or altering other
11 data in the target computer;
12 (e) if, having regard to other methods (if any) of obtaining
13 access to the relevant data which are likely to be as effective,
14 it is reasonable in all the circumstances to do so:
15 (i) using any other computer or a communication in transit
16 to access the relevant data; and
17 (ii) if necessary to achieve that purpose—adding, copying,
18 deleting or altering other data in the computer or the
19 communication in transit;
20 (f) removing a computer or other thing from premises for the
21 purposes of doing any thing specified in the warrant in
22 accordance with this subsection, and returning the computer
23 or other thing to the premises;
24 (g) copying any data to which access has been obtained, and
25 that:
26 (i) appears to be relevant for the purposes of determining
27 whether the relevant data is covered by the warrant; or
28 (ii) is covered by the warrant;
29 (h) intercepting a communication passing over a
30 telecommunications system, if the interception is for the
31 purposes of doing any thing specified in the warrant in
32 accordance with this subsection;
33 (i) using a surveillance device for the purposes of doing any
34 thing specified in the warrant in accordance with this
35 subsection;
36 (j) any other thing reasonably incidental to any of the above.
37 Note: As a result of the warrant, a person who, by means of a
38 telecommunications facility, obtains access to data stored in a
39 computer will not commit an offence under Part 10.7 of the *Criminal*
-

1 *Code* or equivalent State or Territory laws (provided that the person
2 acts within the authority of the warrant).

3 (3) If:

4 (a) a network activity warrant authorises the removal of a
5 computer or other thing from premises as mentioned in
6 paragraph (2)(f); and

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

9 the computer or thing must be returned to the premises as soon as
10 is reasonably practicable to do so once the computer or thing is no
11 longer required for the purposes of doing any thing authorised by
12 the warrant.

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

14 (a) access has been obtained to data; and

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

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

18 *When data is covered by a warrant*

19 (5) For the purposes of this section, data is **covered by** a warrant if
20 access to the data will substantially assist as described in
21 paragraph 27KK(1)(b). To avoid doubt, it is immaterial whether
22 the composition of the group mentioned in that paragraph changes
23 during the period when the warrant is in force.

24 *Certain acts not authorised*

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

27 (a) materially interfere with, interrupt or obstruct:

28 (i) a communication in transit; or

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

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

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

Warrant must provide for certain matters

(7) A network activity warrant must:

- (a) authorise the use of any force against persons and things that is necessary and reasonable to do the things specified in the warrant; and
- (b) if the warrant authorises entering premises—state whether entry is authorised to be made at any time of the day or night or during stated hours of the day or night.

Concealment of access etc.

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

- (a) a network activity warrant; or
- (b) this subsection;

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

- (c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant or under this subsection;
- (d) entering any premises where the computer is reasonably believed to be, for the purposes of doing the things mentioned in paragraph (c);
- (e) entering any other premises for the purposes of gaining entry to or exiting the premises referred to in paragraph (d);
- (f) removing the computer or another thing from any place where it is situated for the purposes of doing the things mentioned in paragraph (c), and returning the computer or other thing to that place;
- (g) if, having regard to other methods (if any) of doing the things mentioned in paragraph (c) which are likely to be as effective, it is reasonable in all the circumstances to do so:
 - (i) using any other computer or a communication in transit to do those things; and
 - (ii) if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;

- 1 (h) intercepting a communication passing over a
2 telecommunications system, if the interception is for the
3 purposes of doing any thing mentioned in this subsection;
4 (i) using a surveillance device, if the use is for the purposes of
5 doing any thing mentioned in this subsection;
6 (j) any other thing reasonably incidental to any of the above;
7 at the following time:
8 (k) at any time while the warrant is in force or within 28 days
9 after it ceases to be in force;
10 (l) if none of the things mentioned in paragraph (c) are done
11 within the 28-day period mentioned in paragraph (k)—at the
12 earliest time after that 28-day period at which it is reasonably
13 practicable to do the things mentioned in paragraph (c).
- 14 (9) Subsection (8) does not authorise the doing of a thing that is likely
15 to:
16 (a) materially interfere with, interrupt or obstruct:
17 (i) a communication in transit; or
18 (ii) the lawful use by other persons of a computer;
19 unless the doing of the thing is necessary to do one or more
20 of the things specified in subsection (8); or
21 (b) cause any other material loss or damage to other persons
22 lawfully using a computer.
- 23 (10) If a computer or another thing is removed from a place in
24 accordance with paragraph (8)(f), the computer or thing must be
25 returned to the place as soon as is reasonably practicable to do so
26 once the computer or thing is no longer required for the purposes
27 of doing any thing mentioned in paragraph (8)(c).

28 **27KQ Extension and variation of network activity warrant**

- 29 (1) If a network activity warrant was issued in response to an
30 application by the chief officer of the Australian Federal Police or
31 the Australian Crime Commission, the chief officer may apply, at
32 any time before the expiry of the warrant:
33 (a) for an extension of the warrant for a period of no more than
34 90 days after the day the warrant would otherwise expire; or
35 (b) for a variation of any of the other terms of the warrant.

- 1 (2) The application is to be made to an eligible Judge or to a
2 nominated AAT member and must be accompanied by the original
3 warrant.
- 4 (3) Sections 27KK and 27KL apply, with any necessary changes, to an
5 application under this section as if it were an application for the
6 warrant.
- 7 (4) The eligible Judge or nominated AAT member may grant an
8 application if satisfied that the matters referred to in
9 subsection 27KM(1) still exist, having regard to the matters in
10 subsection 27KM(2).
- 11 (5) If the eligible Judge or nominated AAT member grants the
12 application, the eligible Judge or nominated AAT member must
13 endorse the new expiry date or the other varied term on the original
14 warrant.
- 15 (6) An application may be made under this section more than once.
- 16 (7) If a network activity warrant is extended or varied in response to an
17 application made by the chief officer of the Australian Federal
18 Police or the Australian Crime Commission, the chief officer must:
19 (a) notify the extension or variation to the Inspector-General of
20 Intelligence and Security; and
21 (b) do so within 7 days after the extension or variation.

22 **27KR Revocation of network activity warrant**

- 23 (1) A network activity warrant may, by instrument in writing, be
24 revoked by an eligible Judge or nominated AAT member on the
25 initiative of the eligible Judge or nominated AAT member at any
26 time before the expiration of the period of validity specified in the
27 warrant.
- 28 (2) If the circumstances set out in subsection 27KS(2) apply in relation
29 to a network activity warrant:
30 (a) if the warrant was issued in response to an application made
31 by the chief officer of the Australian Federal Police—the
32 chief officer of the Australian Federal Police must, by
33 instrument in writing, revoke the warrant; or

- 1 (b) if the warrant was issued in response to an application made
2 by the chief officer of the Australian Crime Commission—
3 the chief officer of the Australian Crime Commission must,
4 by instrument in writing, revoke the warrant.
- 5 (3) The instrument revoking a warrant must be signed by the eligible
6 Judge, the nominated AAT member, the chief officer of the
7 Australian Federal Police or the chief officer of the Australian
8 Crime Commission, as the case requires.
- 9 (4) If an eligible Judge or nominated AAT member revokes a warrant,
10 the eligible Judge or nominated AAT member must give a copy of
11 the instrument of revocation to:
- 12 (a) if the warrant was issued in response to an application made
13 by the chief officer of the Australian Federal Police—the
14 chief officer of the Australian Federal Police; or
15 (b) if the warrant was issued in response to an application made
16 by the chief officer of the Australian Crime Commission—
17 the chief officer of the Australian Crime Commission.
- 18 (5) If:
- 19 (a) an eligible Judge or nominated AAT member revokes a
20 warrant; and
21 (b) at the time of the revocation, a law enforcement officer is
22 executing the warrant;
23 the law enforcement officer is not subject to any civil or criminal
24 liability for any act done in the proper execution of that warrant
25 before the officer is made aware of the revocation.
- 26 (6) If:
- 27 (a) a network activity warrant was issued in response to an
28 application made by the chief officer of the Australian
29 Federal Police or the Australian Crime Commission; and
30 (b) an eligible Judge or nominated AAT member revokes the
31 warrant;
32 the chief officer must:
- 33 (c) notify the revocation to the Inspector-General of Intelligence
34 and Security; and
35 (d) do so within 7 days after the revocation.

(7) If a network activity warrant is revoked by the chief officer of the Australian Federal Police or the Australian Crime Commission, the chief officer must:

- (a) notify the revocation to the Inspector-General of Intelligence and Security; and
- (b) do so within 7 days after the revocation.

27KS Discontinuance of access under warrant

Scope

(1) This section applies if a network activity warrant is issued.

Discontinuance of access

(2) If:

- (a) the warrant was sought by the chief officer of the Australian Federal Police or the Australian Crime Commission; and
- (b) the chief officer is satisfied that access to data under the warrant is no longer required for the purpose referred to in paragraph 27KK(1)(b);

the chief officer must, in addition to revoking the warrant under section 27KR, take the steps necessary to ensure that access to data authorised by the warrant is discontinued.

(3) If:

- (a) the warrant was sought by the chief officer of the Australian Federal Police or the Australian Crime Commission; and
- (b) the chief officer is notified that the warrant has been revoked by an eligible Judge or a nominated AAT member under section 27KR;

the chief officer must take the steps necessary to ensure that access to data authorised by the warrant is discontinued as soon as practicable.

(4) If the law enforcement officer who is primarily responsible for executing the warrant believes that access to data under the warrant is no longer necessary for the purpose referred to in paragraph 27KK(1)(b), the law enforcement officer must immediately inform the chief officer of the law enforcement

1 agency to which the law enforcement officer belongs or is
2 seconded.

3 **27KT Relationship of this Division to parliamentary privileges and**
4 **immunities**

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

- 7 (a) each House of the Parliament;
8 (b) the members of each House of the Parliament;
9 (c) the committees of each House of the Parliament and joint
10 committees of both Houses of the Parliament.

11 **10 Section 41 (paragraph (b) of the definition of *appropriate***
12 ***consenting official*)**

13 Omit “or 43D”, substitute “, 43D or 43E”.

14 **11 At the end of Part 5**

15 Add:

16 **43E Extraterritorial operation of network activity warrants**

- 17 (1) If, before the issue of a network activity warrant, it becomes
18 apparent to the applicant that there will be a need for access to data
19 held in a computer:

- 20 (a) in a foreign country; or
21 (b) on a vessel or aircraft that is registered under the law of a
22 foreign country and that is in or above waters beyond the
23 outer limits of the territorial sea of Australia;

24 the eligible Judge or nominated AAT member considering the
25 application for the warrant must not permit the warrant to authorise
26 that access unless the eligible Judge or nominated AAT member is
27 satisfied that the access has been agreed to by an appropriate
28 consenting official of the foreign country.

- 29 (2) If:

- 30 (a) a network activity warrant has been issued; and
31 (b) after the issue of the warrant, it becomes apparent to the law
32 enforcement officer primarily responsible for executing the

- 1 warrant that there will be a need for access to data held in a
2 computer that is:
- 3 (i) in a foreign country; or
4 (ii) on a vessel or aircraft that is registered under the law of
5 a foreign country and that is in or above waters beyond
6 the outer limits of the territorial sea of Australia;
- 7 the warrant is taken to permit that access if, and only if, the access
8 has been agreed to by an appropriate consenting official of the
9 foreign country.
- 10 (3) Subsections (1) and (2) do not apply to a network activity warrant
11 authorising access to data if:
- 12 (a) the person, or each of the persons, responsible for executing
13 the warrant will be physically present in Australia; and
14 (b) the location where the data is held is unknown or cannot
15 reasonably be determined.
- 16 (4) Despite subsections (1) and (2), if:
- 17 (a) a vessel that is registered under the law of a foreign country
18 is in waters beyond the outer limits of the territorial sea of
19 Australia but not beyond the outer limits of the contiguous
20 zone of Australia; and
21 (b) the relevant offence in respect of which it becomes apparent
22 that access to data held in a computer on the vessel will be
23 required is an offence relating to the customs, fiscal,
24 immigration or sanitary laws of Australia;
- 25 there is no requirement for the agreement of an appropriate
26 consenting official of the foreign country concerned in relation to
27 that access while the vessel is in such waters.
- 28 (5) Despite subsections (1) and (2), if:
- 29 (a) a vessel that is registered under the law of a foreign country
30 is in waters beyond the outer limits of the territorial sea of
31 Australia but not beyond the outer limits of the Australian
32 fishing zone; and
33 (b) the relevant offence in respect of which it becomes apparent
34 that access to data held in a computer on the vessel will be
35 required is an offence against section 100, 100A, 100B, 101,
36 101A or 101AA of the *Fisheries Management Act 1991* or
-

1 section 46A, 46B, 46C, 46D, 49A or 51A of the *Torres Strait*
2 *Fisheries Act 1984*;

3 there is no requirement for the agreement of an appropriate
4 consenting official of the foreign country concerned in relation to
5 that access while the vessel is in those waters.

6 (6) As soon as practicable after the commencement of access to data
7 held in a computer under the authority of a network activity
8 warrant in circumstances where consent to that access is required:

9 (a) in a foreign country; or

10 (b) on a vessel or aircraft that is registered under the law of a
11 foreign country;

12 the chief officer of the law enforcement agency to which the law
13 enforcement officer who applied for the warrant belongs or is
14 seconded must give the Minister evidence in writing that the access
15 has been agreed to by an appropriate consenting official of the
16 foreign country.

17 (7) An instrument providing evidence of the kind referred to in
18 subsection (6) is not a legislative instrument.

19 (8) If a vessel or aircraft that is registered under the laws of a foreign
20 country is in or above the territorial sea of another foreign country,
21 subsections (1) and (2) have effect as if the reference to an
22 appropriate consenting official of the foreign country were a
23 reference to an appropriate consenting official of each foreign
24 country concerned.

25 (9) For the avoidance of doubt, there is no requirement for the
26 agreement of an appropriate consenting official of the foreign
27 country to the access to data held in a computer under the authority
28 of a network activity warrant on a vessel or aircraft of a foreign
29 country that is in Australia or in or above waters within the outer
30 limits of the territorial sea of Australia.

31 **12 Subsection 44(1) (paragraph (a) of the definition of**
32 ***protected information*)**

33 After “warrant”, insert “(other than a network activity warrant)”.

1 **13 Subsection 44(1) (subparagraph (b)(i) of the definition of**
2 ***protected information*)**

3 After “warrant”, insert “(other than a network activity warrant)”.

4 **14 Subsection 44(1) (paragraph (c) of the definition of**
5 ***protected information*)**

6 After “warrant”, insert “(other than a network activity warrant)”.

7 **15 Subsection 44(1) (subparagraph (d)(i) of the definition of**
8 ***protected information*)**

9 After “warrant”, insert “(other than a network activity warrant)”.

10 **16 Subsection 44(1) (subparagraph (d)(iii) of the definition of**
11 ***protected information*)**

12 After “obtained”, insert “(otherwise than purportedly under a network
13 activity warrant)”.

14 **17 Subsection 44(1) (paragraph (d) of the definition of**
15 ***protected information*)**

16 After “warrant” (last occurring), insert “(other than a network activity
17 warrant)”.

18 **18 After section 44**

19 Insert:

20 **44A What is protected network activity warrant information?**

21 For the purposes of this Act, ***protected network activity warrant***
22 ***information*** means:

- 23 (a) any information (other than network activity warrant
24 intercept information) obtained from access to data under a
25 network activity warrant; or
26 (b) any information obtained from the use of a surveillance
27 device under a network activity warrant; or
28 (c) information relating to an application for, the issue of, the
29 existence of, or the expiration of, a network activity warrant;
30 or
31 (d) any information that is likely to enable the identification of:

- 1 (i) a criminal network of individuals specified in a network
2 activity warrant; or
3 (ii) an individual in a criminal network of individuals
4 specified in a network activity warrant; or
5 (iii) a computer specified in a network activity warrant; or
6 (iv) premises specified in a network activity warrant; or
7 (e) any other information obtained by a law enforcement officer:
8 (i) without the authority of a network activity warrant; or
9 (ii) in a case where the information was obtained,
10 purportedly under a network activity warrant, through
11 access to data held in a computer in a foreign country,
12 or on a vessel or aircraft that is registered under the law
13 of a foreign country and that is in or above waters
14 beyond the outer limit of Australia's territorial sea—
15 without the agreement of the appropriate consenting
16 official of that foreign country, and of any other foreign
17 country, whose agreement is required under
18 section 43E;
19 in contravention of the requirement for a network activity
20 warrant.

21 Note: For protection of network activity warrant intercept information, see
22 Part 2-6 of the *Telecommunications (Interception and Access) Act*
23 1979.

24 **19 After section 45A**

25 Insert:

26 **45B Prohibition on use, recording, communication or publication of**
27 **protected network activity warrant information or its**
28 **admission in evidence**

- 29 (1) A person commits an offence if:
30 (a) the person uses, records, communicates or publishes any
31 information; and
32 (b) the information is protected network activity warrant
33 information; and
34 (c) the use, recording, communication or publication of the
35 information is not permitted by this section.

Penalty: Imprisonment for 2 years.

(2) A person commits an offence if:

- (a) the person uses, records, communicates or publishes any information; and
- (b) the information is protected network activity warrant information; and
- (c) the use, recording, communication or publication of the information is not permitted by this section; and
- (d) the use, recording, communication or publication of the information:
 - (i) endangers the health or safety of any person; or
 - (ii) prejudices the effective conduct of an investigation into a relevant offence.

Penalty: Imprisonment for 10 years.

(3) Subject to subsections (4), (5), (7) and (10), protected network activity warrant information may not be admitted in evidence in any proceedings.

(4) Subsections (1), (2) and (3) do not apply to:

- (a) the use, recording, communication or publication of protected network activity warrant information in connection with the administration or execution of this Act; or
- (b) the use, recording, communication or publication of any information that has been disclosed in proceedings in open court lawfully; or
- (c) the use or communication of protected network activity warrant information by a person who believes on reasonable grounds that the use or communication is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property; or
- (d) the communication to the Director-General (within the meaning of the *Australian Security Intelligence Organisation Act 1979*) of protected network activity warrant information that relates or appears to relate to any matter within the functions of that organisation; or
- (e) the communication to the agency head (within the meaning of the *Intelligence Services Act 2001*) of an agency (within

- 1 the meaning of that Act) of protected network activity
2 warrant information that relates or appears to relate to any
3 matter within the functions of that agency; or
4 (f) the use, recording or communication of:
5 (i) protected network activity warrant information referred
6 to in paragraph (d)—by the Director-General (within the
7 meaning of the *Australian Security Intelligence*
8 *Organisation Act 1979*), an ASIO employee (within the
9 meaning of that Act) or an ASIO affiliate (within the
10 meaning of that Act); or
11 (ii) protected network activity warrant information referred
12 to in paragraph (e)—by the agency head (within the
13 meaning of the *Intelligence Services Act 2001*), or a
14 staff member (within the meaning of that Act), of an
15 agency (within the meaning of that Act);
16 in the performance of the official functions of the
17 Director-General, ASIO employee, ASIO affiliate, agency
18 head or staff member, as the case may be.
- 19 (5) Protected network activity warrant information (other than
20 information that was obtained from the use of a surveillance device
21 under a network activity warrant) may be used, recorded,
22 communicated or published, or may be admitted in evidence, if it is
23 necessary to do so for any of the following purposes:
24 (a) the purposes of the Australian Federal Police collecting,
25 correlating, analysing or disseminating criminal intelligence
26 in the performance of the functions conferred by section 8 of
27 the *Australian Federal Police Act 1979*;
28 (b) the purposes of the Australian Crime Commission collecting,
29 correlating, analysing or disseminating criminal intelligence
30 in the performance of the functions conferred by section 7A
31 of the *Australian Crime Commission Act 2002*;
32 (c) the purposes of the Australian Federal Police or the
33 Australian Crime Commission making reports in relation to
34 criminal intelligence;
35 (d) the making of an application for a warrant;
36 (e) the making of an application for the variation of a warrant;
37 (f) the making of an application for the extension of a warrant;

- 1 (g) the keeping of records and the making of reports by the
2 Australian Federal Police or the Australian Crime
3 Commission under Division 2;
4 (h) the purposes of an IGIS official exercising powers, or
5 performing functions or duties, as an IGIS official;
6 (i) the purposes of an investigation of an offence against
7 subsection (1) or (2);
8 (j) a proceeding relating to an offence against subsection (1) or
9 (2).
- 10 (6) The definition of **warrant** in subsection 6(1) does not apply to
11 paragraphs (5)(d), (e) and (f) of this section.
12 Note: This means that warrant has its ordinary meaning.
- 13 (7) Protected network activity warrant information that was obtained
14 from the use of a surveillance device under a network activity
15 warrant may be used, recorded, communicated or published, or
16 may be admitted in evidence, if it is necessary to do so for any of
17 the following purposes:
18 (a) the purposes of doing a thing authorised by a network
19 activity warrant;
20 (b) the purposes of an IGIS official exercising powers, or
21 performing functions or duties, as an IGIS official;
22 (c) the purposes of an investigation of an offence against
23 subsection (1) or (2);
24 (d) a proceeding relating to an offence against subsection (1) or
25 (2).
- 26 (8) Protected network activity warrant information may be
27 communicated by an Ombudsman official to an IGIS official for
28 the purposes of the IGIS official exercising powers, or performing
29 functions or duties, as an IGIS official.
- 30 (9) Protected network activity warrant information may be
31 communicated by an IGIS official to an Ombudsman official for
32 the purposes of the Ombudsman official exercising powers, or
33 performing functions or duties, as an Ombudsman official.
- 34 (10) Protected network activity warrant information may be admitted in
35 evidence in:
-

1 (a) a criminal proceeding for an offence against subsection (1) or
2 (2); or

3 (b) a proceeding that is not a criminal proceeding.

4 (11) If:

5 (a) protected network activity warrant information was obtained
6 from access to data, or the use of a surveillance device, under
7 a network activity warrant; and

8 (b) the warrant was granted in response to an application made
9 by the chief officer of a particular law enforcement agency;
10 and

11 (c) the information:

12 (i) is communicated to another law enforcement agency
13 (by communicating it to the chief officer or another
14 officer of that agency) for a particular purpose; or

15 (ii) is communicated to any agency that is not a law
16 enforcement agency (other than the Office of the
17 Inspector-General of Intelligence and Security, the
18 Australian Security Intelligence Organisation and the
19 agencies within the meaning of the *Intelligence Services*
20 *Act 2001*) (by communicating it to the officer in charge
21 of that agency or to another officer of that agency) for a
22 particular purpose;

23 the information that has been so communicated:

24 (d) may be communicated from one officer to another within that
25 agency for that purpose only; and

26 (e) must not be communicated to any person who is not an
27 officer of that agency.

28 **20 After section 46**

29 Insert:

30 **46AA Dealing with records obtained by accessing data under a**
31 **network activity warrant**

32 (1) The chief officer of the Australian Federal Police or the Australian
33 Crime Commission:

34 (a) must ensure that every record or report comprising:

35 (i) protected network activity warrant information; or

- 1 (ii) network activity warrant intercept information;
2 is kept in a secure place that is not accessible to people who
3 are not entitled to deal with the record or report; and
4 (b) must cause to be destroyed any record or report referred to in
5 paragraph (a):
6 (i) as soon as practicable after the making of the record or
7 report if the chief officer is satisfied that no civil or
8 criminal proceeding to which the material contained in
9 the record or report relates has been, or is likely to be,
10 commenced and that the material contained in the
11 record or report is not likely to be required in
12 connection with an activity referred to in
13 subsection 45B(4) or a purpose referred to in
14 subsection 45B(5) or (7); and
15 (ii) within the period of 5 years after the making of the
16 record or report, and within each period of 5 years
17 thereafter, unless, before the end of that period, the chief
18 officer is satisfied in relation to the material contained
19 in the record or report of a matter referred to in
20 subparagraph (i) and certifies to that effect.
- 21 (2) If an agency is not a law enforcement agency but, as described in
22 subsection 45B(5) or (7), receives records or reports obtained by
23 accessing data, or using a surveillance device, under a network
24 activity warrant, the officer in charge of the agency:
25 (a) must ensure that every record or report that is so received is
26 kept in a secure place that is not accessible to people who are
27 not entitled to deal with the record or report; and
28 (b) must cause to be destroyed any record or report referred to in
29 paragraph (a):
30 (i) as soon as practicable after the receipt of the record or
31 report by the agency if the officer in charge is satisfied
32 that no civil or criminal proceeding to which the
33 material contained in the record or report relates has
34 been, or is likely to be, commenced and that the material
35 contained in the record or report is not likely to be
36 required in connection with an activity referred to in
37 subsection 45B(4) or a purpose referred to in
38 subsection 45B(5) or (7); and

- 1 (ii) within the period of 5 years after the making of the
2 record or report, and within each period of 5 years
3 thereafter, unless, before the end of that period, the
4 officer in charge is satisfied in relation to the material
5 contained in the record or report of a matter referred to
6 in subparagraph (i) and certifies to that effect.

- 7 (3) Subsection (2) does not apply to the Office of the
8 Inspector-General of Intelligence and Security.

9 **21 Subsection 47A(7) (after paragraph (c) of the definition of**
10 **computer access technologies or methods)**

11 Insert:

- 12 (ca) a network activity warrant; or

13 **22 After subsection 49(2D)**

14 Insert:

- 15 (2E) In the case of a network activity warrant for access to data held in a
16 computer, the report must:

- 17 (a) state whether the warrant was executed; and

- 18 (b) if so:

- 19 (i) state the name of the person primarily responsible for
20 the execution of the warrant; and

- 21 (ii) state the name of each person involved in accessing data
22 under the warrant; and

- 23 (iii) state the period during which the data was accessed; and

- 24 (iv) state the name, if known, of any person whose data was
25 accessed; and

- 26 (v) give details of any premises, if known, at which the
27 computer was located; and

- 28 (vi) give details of any use of a surveillance device under the
29 warrant; and

- 30 (vii) give details of the extent to which the execution of the
31 warrant has contributed to the prevention, detection or
32 frustration of one or more kinds of relevant offences;
33 and

- (viii) give details of the extent to which the execution of the warrant has assisted the agency in carrying out its functions; and
- (ix) give details of the communication of information obtained by accessing data under the warrant to persons other than officers of the agency; and
- (x) give details of the compliance with the conditions (if any) to which the warrant was subject; and
- (xi) give details of the information that was obtained from access to data under the warrant; and
- (xii) give details of how the information that was obtained under the warrant was used; and
- (xiii) give details of whether the information that was obtained under the warrant was destroyed or retained under section 46AA; and
- (xiv) give details of any premises accessed, telecommunications intercepted or computers removed from premises under the warrant; and
- (xv) give details of any activities undertaken under subsection 27KP(8) in relation to the warrant; and
- (xvi) give details of any assistance orders made under subsection 64A(6A) in relation to the warrant; and
- (c) if the warrant was extended or varied, state:
- (i) the number of extensions or variations; and
- (ii) the reasons for them.

23 After section 49C

Insert:

49D Notification to Inspector-General of Intelligence and Security of things done under a network activity warrant

If:

- (a) a network activity warrant was issued in response to an application made by the chief officer of the Australian Federal Police or the Australian Crime Commission; and

- 1 (b) a thing mentioned in subsection 27KP(8) was done under the
2 warrant after the 28-day period mentioned in
3 paragraph 27KP(8)(k);
4 the chief officer must:
5 (c) notify the Inspector-General of Intelligence and Security of
6 the fact that the thing was done under the warrant after the
7 28-day period mentioned in paragraph 27KP(8)(k); and
8 (d) do so within 7 days after the thing was done.

9 **24 After paragraph 50(1)(eb)**

10 Insert:

- 11 (ec) if the agency is the Australian Federal Police or the
12 Australian Crime Commission—the kinds of offences in
13 relation to which information was obtained under network
14 activity warrants issued during that year in response to
15 applications made by the chief officer of the agency; and

16 **25 Paragraph 51(b)**

17 Omit “or 27KG(4)”, substitute “, 27KG(4) or 27KR(4)”.

18 **26 After paragraph 52(1)(h)**

19 Insert:

- 20 (ha) if the agency is the Australian Federal Police or the
21 Australian Crime Commission—details of things done under
22 subsection 27KP(8) in relation to a network activity warrant;

23 **27 Paragraph 52(1)(j)**

24 After “46(1)(b)”, insert “or 46AA(1)(b)”.

25 **28 After subsection 55(1)**

26 Insert:

- 27 (1A) Subsection (1) does not apply to compliance with:
28 (a) Division 6 of Part 2 (network activity warrants); or
29 (b) the remaining provisions of this Act so far as they relate to
30 network activity warrants.

29 At the end of subsection 62(1)

Add:

; or (e) anything done by the law enforcement officer in connection with:

- (i) the communication by a person to another person; or
 - (ii) the making use of; or
 - (iii) the making of a record of; or
 - (iv) the custody of a record of;
- information obtained from access to data under a network activity warrant.

30 After subparagraph 64A(1)(a)(i)

Insert:

- (ia) a network activity warrant; or

31 After subsection 64A(6)

Insert:

Network activity warrant

(6A) In the case of a computer that is the subject of a network activity warrant, the eligible Judge or nominated AAT member may grant the assistance order if the eligible Judge or nominated AAT member is satisfied that:

- (a) there are reasonable grounds for suspecting that access to data held in the computer will substantially assist in the collection of intelligence that:
 - (i) relates to the group referred to in paragraph 27KK(1)(a) or to any of the individuals in the group; and
 - (ii) is relevant to the prevention, detection or frustration of one or more kinds of relevant offences; and
- (b) the specified person is:
 - (i) reasonably suspected of having committed any of the relevant offences in respect of which the warrant was issued; or
 - (ii) the owner or lessee of the computer; or
 - (iii) an employee of the owner or lessee of the computer; or

- (iv) a person engaged under a contract for services by the owner or lessee of the computer; or
- (v) a person who uses or has used the computer; or
- (vi) a person who is or was a system administrator for the system including the computer; and
- (c) the specified person has relevant knowledge of:
 - (i) the computer or a computer network of which the computer forms or formed a part; or
 - (ii) measures applied to protect data held in the computer.

31A After subsection 64A(7)

Insert:

- (7A) In determining whether the assistance order should be granted, the eligible Judge or nominated AAT member must have regard to whether the specified person is, or has been, subject to:
 - (a) another order under this section; or
 - (b) an order under section 64B of this Act; or
 - (c) an order under section 3LA or 3ZZVG of the *Crimes Act 1914*;so far as that matter is known to the eligible Judge or nominated AAT member.
- (7B) Subsection (7A) does not limit the matters to which the eligible Judge or nominated AAT member may have regard.

Duration of assistance order

- (7C) If an assistance order is granted in relation to a computer that is the subject of a computer access warrant or a network activity warrant, the order ceases to be in force when the warrant ceases to be in force.
- (7D) If an assistance order is granted in relation to a computer that is the subject of an emergency authorisation given in response to an application under subsection 28(1A), 29(1A) or 30(1A), the order ceases to be in force when the emergency authorisation ceases to be in force.

1 *Protection from civil liability*

2 (7E) A person is not subject to any civil liability in respect of an act
3 done by the person:

4 (a) in compliance with an assistance order; or

5 (b) in good faith in purported compliance with an assistance
6 order.

7 **32 Paragraph 65(1A)(a)**

8 After “data disruption warrant”, insert “, network activity warrant”.

Part 2—Consequential amendments

Australian Crime Commission Act 2002

33 Subsection 51(4) (at the end of the definition of *relevant Act*)

Add:

; or (e) the *Inspector-General of Intelligence and Security Act 1986*, or any other Act, or instrument made under an Act, that confers functions, duties or powers on the Inspector-General of Intelligence and Security.

34 After paragraph 59AA(1B)(f)

Insert:

(fa) the Inspector-General of Intelligence and Security;

Australian Federal Police Act 1979

35 Subsection 4(1)

Insert:

IGIS official means:

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

36 Subsection 40ZA(3)

Omit “and (6)”, substitute “, (6) and (6A)”.

37 After subsection 40ZA(6)

Insert:

(6A) Subsection (2) does not prevent a person from making a record of, or divulging or communicating, information for the purpose of an IGIS official exercising powers, or performing functions or duties, as an IGIS official.

1 **38 After paragraph 60A(2)(f)**

2 Insert:

3 ; or (g) the purposes of an IGIS official carrying out, performing or
4 exercising any of the IGIS official's duties, functions or
5 powers as an IGIS official.

6 ***Australian Human Rights Commission Act 1986***

7 **39 Subsection 3(1)**

8 Insert:

9 *ACIC* means the agency known as the Australian Criminal
10 Intelligence Commission established by the *Australian Crime*
11 *Commission Act 2002*.

12 *examiner* of ACIC means an examiner within the meaning of the
13 *Australian Crime Commission Act 2002*.

14 *IGIS official* means:

- 15 (a) the Inspector-General of Intelligence and Security; or
16 (b) any other person covered by subsection 32(1) of the
17 *Inspector-General of Intelligence and Security Act 1986*.

18 **40 At the end of subsection 11(3)**

19 Add:

20 Note: Both the Commission and the Inspector-General of Intelligence and
21 Security have functions in relation to ACIC and the Australian Federal
22 Police. The Commission and the Inspector-General can transfer
23 matters between each other and share information in relation to
24 actions taken by any of those agencies (see subsection 20(4C),
25 section 46PZ and subsection 49(4C) of this Act, and Part IIIA of the
26 *Inspector-General of Intelligence and Security Act 1986*).

27 **41 At the end of subsection 20(1)**

28 Add:

29 Note: A complaint is taken to have been made to the Commission if all or
30 part of a complaint is transferred to the Commission under
31 section 32AD of the *Inspector-General of Intelligence and Security*
32 *Act 1986* (see section 46PZ of this Act).

1 **42 After subsection 20(4B)**

2 Insert:

3 (4C) If:

- 4 (a) a complaint has been made to the Commission in relation to:
- 5 (i) an act or practice of ACIC (except an act or practice of
- 6 an examiner of ACIC performing functions and
- 7 exercising powers as an examiner); or
- 8 (ii) an act or practice of the Australian Federal Police; and
- 9 (b) because the Commission is of the opinion that the subject
- 10 matter of the complaint could be more effectively or
- 11 conveniently dealt with by the Inspector-General of
- 12 Intelligence and Security under the *Inspector-General of*
- 13 *Intelligence and Security Act 1986*, the Commission decides
- 14 not to inquire, or not to continue to inquire, into that act or
- 15 practice;

16 the Commission must:

- 17 (c) consult the Inspector-General in relation to transferring the
- 18 complaint or part of the complaint; and
- 19 (d) if the Inspector-General agrees to the transfer of the
- 20 complaint or part of the complaint—transfer the complaint or
- 21 part to the Inspector-General as soon as is reasonably
- 22 practicable; and
- 23 (e) as soon as is reasonably practicable, take reasonable steps to
- 24 give notice in writing to the complainant stating that the
- 25 complaint or part has been so transferred; and
- 26 (f) give to the Inspector-General any information or documents
- 27 that relate to the complaint or part and are in the possession,
- 28 or under the control, of the Commission.

29 (4D) Without limiting subsection (4C), the Commission may consult

30 with, and obtain an agreement from, the Inspector-General of

31 Intelligence and Security by entering into an arrangement with the

32 Inspector-General relating to the transfer of complaints (or parts)

33 generally.

34 **43 Subsection 46P(1) (note)**

35 Omit “Note”, substitute “Note 1”.

1 **44 At the end of subsection 46P(1)**

2 Add:

3 Note 2: Under section 46PZ, a complaint may be taken to be lodged with the
4 Commission if all or part of a complaint is transferred from the
5 Inspector-General of Intelligence and Security under section 32AD of
6 the *Inspector-General of Intelligence and Security Act 1986*.

7 **45 Before section 47**

8 Insert:

9 **46PZ Transfer of complaints from the Inspector-General of**
10 **Intelligence and Security**

11 (1) If the Inspector-General of Intelligence and Security transfers all or
12 part of a complaint to the Commission under section 32AD of the
13 *Inspector-General of Intelligence and Security Act 1986*, in respect
14 of an act or practice of ACIC or the Australian Federal Police, the
15 Commission may determine, in writing, that a complaint is taken to
16 have been:

- 17 (a) made as referred to in paragraph 20(1)(b) of this Act; or
18 (b) lodged under section 46P of this Act.

19 Note: The Commission may also transfer a complaint or part of a complaint
20 to the Inspector-General of Intelligence and Security under
21 subsection 20(4C).

22 (2) The determination has effect accordingly.

23 (3) The determination is not a legislative instrument.

24 **46 Subsection 49(4A)**

25 After “20(4A)(e)”, insert “or (4C)(f)”.

26 **47 After subsection 49(4B)**

27 Insert:

28 (4C) Subsection (1) does not prevent the Commission, or a person
29 acting for or on behalf of the Commission, from giving information
30 or documents to an IGIS official for the purpose of the IGIS
31 official exercising a power, or performing a function or duty, as an
32 IGIS official.

Note: A defendant bears an evidential burden in relation to a matter in subsection (4C) (see subsection 13.3(3) of the *Criminal Code*).

Australian Information Commissioner Act 2010

48 Section 3

Insert:

IGIS official has the meaning given by subsection 29(6).

49 After paragraph 29(2)(c)

Insert:

; or (d) the person:

- (i) records or otherwise uses the information for the purpose of an IGIS official exercising a power, or performing a function or duty, as an IGIS official; or
- (ii) discloses the information to an IGIS official for the purpose of the IGIS official exercising a power, or performing a function or duty, as an IGIS official.

50 At the end of section 29

Add:

(6) In this Act:

IGIS official means:

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

Inspector-General of Intelligence and Security Act 1986

51 Subsection 3(1)

Insert:

ACIC means the agency known as the Australian Criminal Intelligence Commission established by the *Australian Crime Commission Act 2002*.

CEO of ACIC means the Chief Executive Officer of ACIC.

1 **52 Subsection 3(1) (after paragraph (d) of the definition of**
2 **head)**

3 Insert:

- 4 (e) in relation to ACIC—the CEO of ACIC; or
5 (ea) in relation to the Australian Federal Police—the
6 Commissioner of Police; or

7 **53 Subsection 3(1)**

8 Insert:

9 **Information Commissioner:** see section 3A of the *Australian*
10 *Information Commissioner Act 2010*.

11 **Inspector-General ADF** means the Inspector-General of the
12 Australian Defence Force referred to in section 110B of the
13 *Defence Act 1903*.

14 **integrity body:**

- 15 (a) means any of the following:
16 (i) the Ombudsman;
17 (ii) the Australian Human Rights Commission;
18 (iii) the Information Commissioner;
19 (iv) the Integrity Commissioner;
20 (v) the Inspector-General ADF; and
21 (b) for a complaint—has the meaning given by
22 paragraph 11(4A)(a).

23 **Integrity Commissioner** has the meaning given by section 5 of the
24 *Law Enforcement Integrity Commissioner Act 2006*.

25 **54 Subsection 3(1) (definition of *intelligence agency*)**

26 Repeal the definition, substitute:

27 ***intelligence agency*** means:

- 28 (a) ASIO, ASIS, AGO, DIO, ASD or ONI; or
29 (b) the following agencies that have an intelligence function:
30 (i) the Australian Federal Police;
31 (ii) ACIC.
-

1 **55 Subsection 3(1)**

2 Insert:

3 ***intelligence function:***

4 (a) for ACIC—means:

- 5 (i) the collection, correlation, analysis, production and
6 dissemination of intelligence obtained by ACIC from
7 the execution of a network activity warrant; or
8 (ii) the performance of a function, or the exercise of a
9 power, conferred on a law enforcement officer of ACIC
10 by the network activity warrant provisions of the
11 *Surveillance Devices Act 2004*; or

12 (b) for the Australian Federal Police—means:

- 13 (i) the collection, correlation, analysis, production and
14 dissemination of intelligence obtained by the Australian
15 Federal Police from the execution of a network activity
16 warrant; or
17 (ii) the performance of a function, or the exercise of a
18 power, conferred on a law enforcement officer of the
19 Australian Federal Police by the network activity
20 warrant provisions of the *Surveillance Devices Act*
21 *2004*.

22 ***law enforcement officer***, when used in relation to the Australian
23 Federal Police or ACIC, has the same meaning as in the
24 *Surveillance Devices Act 2004*.

25 ***network activity warrant*** has the same meaning as in the
26 *Surveillance Devices Act 2004*.

27 ***network activity warrant provisions of the Surveillance Devices***
28 ***Act 2004*** means:

- 29 (a) Division 6 of Part 2 of that Act; or
30 (b) the remaining provisions of that Act so far as they relate to
31 network activity warrants.

32 **56 After subsection 8(3)**

33 Insert:

- 1 (3A) Subject to this section, the functions of the Inspector-General in
2 relation to ACIC or the Australian Federal Police are:
- 3 (a) at the request of the Attorney-General or the responsible
4 Minister; or
- 5 (b) of the Inspector-General's own motion; or
- 6 (c) in response to a complaint made to the Inspector-General;
7 to inquire into any of the following matters, to the extent that the
8 matter relates to an intelligence function of that agency:
- 9 (d) the compliance by that agency with the laws of the
10 Commonwealth and of the States and Territories;
- 11 (e) the compliance by that agency with directions or guidelines
12 given to that agency by the responsible Minister;
- 13 (f) the propriety of particular activities of that agency;
- 14 (g) the effectiveness and appropriateness of the procedures of
15 that agency relating to the legality or propriety of the
16 activities of that agency;
- 17 (h) any matter that relates to an act or practice of that agency,
18 referred to the Inspector-General by the Australian Human
19 Rights Commission:
- 20 (i) that is or may be inconsistent with or contrary to any
21 human right; or
- 22 (ii) that constitutes or may constitute discrimination; or
- 23 (iii) that is or may be unlawful under the *Age Discrimination*
24 *Act 2004*, the *Disability Discrimination Act 1992*, the
25 *Racial Discrimination Act 1975* or the *Sex*
26 *Discrimination Act 1984*;
- 27 (i) in relation to ACIC—the compliance by that agency with:
- 28 (i) directions or guidelines given to that agency; or
- 29 (ii) policies or other decisions made;
30 by the Board of ACIC or the Inter-Governmental Committee
31 established under the *Australian Crime Commission Act*
32 *2002*.
- 33 (3B) The functions of the Inspector-General under subsection (3A) do
34 not include inquiring into any action taken by an examiner (within
35 the meaning of the *Australian Crime Commission Act 2002*) of
36 ACIC in performing functions or exercising powers as an
37 examiner.
-

1 **57 Subsection 8(5)**

2 Omit “and (3)”, substitute “, (3) and (3A)”.

3 **58 Subsection 8(5)**

4 After “DIO”, insert “, ACIC, the Australian Federal Police”.

5 **59 Paragraph 8A(1)(b)**

6 Omit “intelligence agency”, substitute “intelligence agency (within the
7 meaning of this Act); and”.

8 **60 After paragraph 8A(1)(b)**

9 Insert:

10 (c) if the intelligence agency is ACIC or the Australian Federal
11 Police—the conduct relates to that agency’s intelligence
12 functions;

13 **61 Subsection 8A(1)**

14 After “so relates”, insert “as described in paragraph (b)”.

15 **62 Paragraph 9AA(b)**

16 Omit “paragraph 8(1)(d)”, substitute “paragraphs 8(1)(d) and (3A)(b)”.

17 **63 After paragraph 9AA(b)**

18 Insert:

19 (ba) inquire into action taken by the Board of ACIC or the
20 Inter-Governmental Committee established under the
21 *Australian Crime Commission Act 2002* except to the extent
22 necessary to perform the functions of the Inspector-General
23 referred to in paragraph 8(3A)(f); or

24 **64 Section 9A**

25 Before “The functions”, insert “(1)”.

26 **65 At the end of section 9A**

27 Add:

28 (2) For the purposes of conducting an inspection of an intelligence
29 agency under subsection (1) in a case where the agency is ACIC or

1 the Australian Federal Police, the Inspector-General or a member
2 of staff assisting the Inspector-General referred to in
3 paragraph 32(1)(a):

- 4 (a) may, at all reasonable times, enter and remain on any
5 premises (including any land or place); and
6 (b) is entitled to all reasonable facilities and assistance that the
7 head of the agency is capable of providing; and
8 (c) is entitled to full and free access at all reasonable times to
9 any information, documents or other property of the agency;
10 and
11 (d) may examine, make copies of or take extracts from any
12 information or documents.

13 **66 At the end of subsection 10(1)**

14 Add:

- 15 Note 1: A complaint is taken to have been made under this Act if all or part of
16 the complaint is transferred to the Inspector-General by an integrity
17 body (see section 32AE of this Act).
18 Note 2: See also Part IIIA which deals with relationships with other agencies
19 and information sharing.

20 **67 Before subsection 11(2)**

21 Insert:

22 *When inquiry or further inquiry into complaints is not required*

23 **68 After subsection 11(4)**

24 Insert:

- 25 (4A) Without limiting paragraph (2)(c), the Inspector-General may
26 decide not to inquire into, or not to inquire further into, a complaint
27 or part of a complaint in relation to action taken by an intelligence
28 agency if:
29 (a) a complaint in respect of the action has been, or could have
30 been, made by the complainant to any of the following
31 persons or bodies (the *integrity body* for the complaint):
32 (i) the Ombudsman;
33 (ii) the Australian Human Rights Commission, under
34 Division 3 of Part II (human rights complaints) or

- 1 Part IIB (unlawful discrimination complaints) of the
2 *Australian Human Rights Commission Act 1986*;
3 (iii) the Information Commissioner under Part V of the
4 *Privacy Act 1988*;
5 (iv) the Integrity Commissioner;
6 (v) the Inspector-General ADF; and
7 (b) the Inspector-General is satisfied that the subject matter of
8 the complaint or the part of the complaint could be more
9 effectively or conveniently dealt with by the integrity body
10 for the complaint.

11 Note: The complaint or part of the complaint may be transferred to the
12 integrity body for the complaint under section 32AD.

13 *Inquiries into complaints about employment, contracts and related*
14 *matters*

15 **69 Paragraph 15(3)(a)**

16 After “ASD” (wherever occurring), insert “, ACIC, the Australian
17 Federal Police”.

18 **70 Paragraph 21(1B)(a)**

19 After “ASD” (wherever occurring), insert “, ACIC, the Australian
20 Federal Police”.

21 **71 After Part III**

22 Insert:

23 **Part IIIA—Relationships with other agencies and** 24 **information sharing** 25

26 **32AC Information sharing with integrity bodies**

- 27 (1) The Inspector-General may share information or documents with
28 an integrity body (the *receiving body*) if:
29 (a) the information or documents are obtained by the
30 Inspector-General in the course of exercising powers, or

- 1 performing functions or duties, in relation to ACIC or the
2 Australian Federal Police; and
3 (b) the information or documents are relevant to the receiving
4 body's functions; and
5 (c) the Inspector-General is satisfied on reasonable grounds that
6 the receiving body has satisfactory arrangements in place for
7 protecting the information or documents.
- 8 (2) To avoid doubt, the Inspector-General may share information or
9 documents with an integrity body whether or not the
10 Inspector-General is transferring a complaint or part of a complaint
11 to the integrity body.
- 12 (3) Without limiting paragraph (1)(c), the Inspector-General may make
13 arrangements with the head of an intelligence agency in relation to
14 protecting information or documents provided to the
15 Inspector-General by the agency.

32AD Transferring complaints to other integrity bodies

17 If the Inspector-General decides under subsection 11(4A) not to
18 inquire into, or not to inquire further into, a complaint or part of a
19 complaint in relation to action taken by an intelligence agency, the
20 Inspector-General may transfer all or part of the complaint to the
21 integrity body for the complaint.

22 Note: The complaint is taken to have been made under the Act establishing
23 the integrity body (see sections 46PZ of the *Australian Human Rights*
24 *Commission Act 1986*, 23A of the *Law Enforcement Integrity*
25 *Commissioner Act 2006*, 5B of the *Ombudsman Act 1976* and 49B of
26 the *Privacy Act 1988*).

32AE Complaints transferred by integrity bodies

28 For the purposes of this Act, a complaint is taken to have been
29 made to the Inspector-General under this Act if all or part of the
30 complaint is transferred (however described) to the
31 Inspector-General by an integrity body.

32 Note: Complaints may be transferred to the Inspector-General under
33 subsections 20(4C) of the *Australian Human Rights Commission Act*
34 *1986*, 6F(3) of the *Ombudsman Act 1976* and 50(3) of the *Privacy Act*
35 *1988*, and paragraph 110C(3)(b) of the *Defence Act 1903*.

72 At the end of subsection 32A(1)

Add:

- ; (e) in the case of ACIC or the Australian Federal Police:
- (i) a report given to the Minister under section 46 of the *Public Governance, Performance and Accountability Act 2013*; or
 - (ii) any other report prepared on a periodic basis, and given to the responsible Minister, that the Inspector-General is satisfied relates to the performance by ACIC or the Australian Federal Police of its intelligence functions;
- (f) in the case of ACIC—a report that:
- (i) is provided to the Board of ACIC or to the Inter-Governmental Committee established under the *Australian Crime Commission Act 2002*; and
 - (ii) the Inspector-General is satisfied relates to the performance by ACIC of its intelligence functions;
- if the report was prepared:
- (iii) by the CEO of ACIC; or
 - (iv) by the Chair of the Board and is in the possession of ACIC.

73 After paragraph 32A(5)(a)

Insert:

- (aa) in the case of ACIC or the Australian Federal Police, the head of the agency has not provided the responsible Minister with a copy of a report mentioned in subparagraph (1)(e)(i); or

74 At the end of section 32A

Add:

- (6) In the case of ACIC, if the CEO of ACIC or the Chair of the Board (as the case requires) has not given the Board or the Inter-Governmental Committee established under the *Australian Crime Commission Act 2002* a copy of a report mentioned in paragraph (1)(f), the CEO or Chair need not give a copy of the report to the Inspector-General until the report has been given to

1 the Board or the Inter-Governmental Committee (as the case
2 requires).

3 **75 Subsections 32B(2) and (4)**

4 Repeal the subsections, substitute:

5 (1A) This section also applies to any guidelines or directions:

6 (a) that relate to the performance by ACIC or the Australian
7 Federal Police of that agency's intelligence functions; and

8 (b) that are given:

9 (i) by the responsible Minister to the head of ACIC or the
10 Australian Federal Police; or

11 (ii) to ACIC by the Board of ACIC or by the
12 Inter-Governmental Committee established under the
13 *Australian Crime Commission Act 2002*.

14 (2) As soon as practicable after a direction or guideline is given to the
15 head of that agency, the Inspector-General must be given a copy of
16 the direction or guideline by:

17 (a) the Minister; or

18 (b) for directions or guidelines referred to in
19 subparagraph (1A)(b)(ii)—the CEO of ACIC.

20 **76 After section 34B**

21 Insert:

22 **34C No evidential burden for IGIS officials in relation to defences to**
23 **secrecy offences**

24 (1) Despite subsections 13.3(2) and (3) of the *Criminal Code*, in a
25 prosecution for any offence of:

26 (a) disclosing, making a record of, or using, information or a
27 document; or

28 (b) causing information or a document to be disclosed, recorded
29 or used;

30 an IGIS official does not bear an evidential burden in relation to
31 whether the disclosure, record or use is for the purposes of, or in
32 connection with, that or any other IGIS official exercising a power,
33 or performing a function or duty, as an IGIS official.

(2) Subsection (1) applies even if the offence referred to in that subsection has additional physical elements to those referred to in paragraph (1)(a) or (b).

(3) To avoid doubt:

(a) an offence may be covered by subsection (1) even if the offence does not refer to disclosing, making a record of, or using, information or a document; and

(b) without limiting paragraph (a):

(i) disclosing information or a document includes communicating information or a document; and

(ii) making a record of information or a document includes reproducing information or a document; and

(iii) using information or a document includes dealing with, reading or examining information or a document.

Law Enforcement Integrity Commissioner Act 2006

77 Subsection 5(1)

Insert:

IGIS official means:

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

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

78 Subsection 5(1) (paragraph (b) of the definition of *law enforcement secrecy provision*)

Omit “section 45”, substitute “sections 45 and 45B”.

79 After section 23

Insert:

23A Transfer of complaints from the Inspector-General of Intelligence and Security

If:

(a) the Inspector-General of Intelligence and Security transfers all or part of a complaint to the Integrity Commissioner under

1 section 32AD of the *Inspector-General of Intelligence and*
2 *Security Act 1986*; and

3 (b) the complaint or the part of the complaint involves an
4 allegation, or information, that raises a corruption issue;
5 the person who made the complaint is taken to have referred the
6 allegation or information to the Integrity Commissioner under
7 subsection 23(1).

8 **80 After subsection 90(3A)**

9 Insert:

10 *Disclosure to IGIS officials*

11 (3B) Nothing in a direction given by the Integrity Commissioner
12 prevents:

13 (a) a person from disclosing hearing material to an IGIS official;
14 or

15 (b) an IGIS official using hearing material, for the purpose of the
16 IGIS official performing a function, or exercising a power, as
17 an IGIS official; or

18 (c) an IGIS official disclosing hearing material to a person who
19 is not an IGIS official if the hearing material could be
20 disclosed to the person under paragraph (1)(b).

21 (3C) However, if the Commissioner is satisfied that the disclosure or use
22 would be reasonably likely to prejudice the performance of
23 functions, or the exercise of powers, of the Integrity
24 Commissioner, the Integrity Commissioner may direct under
25 subsection (1) that subsection (3B) does not apply.

26 (3D) The Integrity Commissioner must consult the Inspector-General of
27 Intelligence and Security as soon as practicable after giving a
28 direction under subsection (1) in accordance with subsection (3C).

29 **81 After paragraph 208(3)(a)**

30 Insert:

31 (aa) the Inspector-General of Intelligence and Security;

1 **82 Subsection 208(7)**

2 After “or (6)”, insert “(except to the Inspector-General of Intelligence
3 and Security for the purpose of performing the Inspector-General’s
4 functions)”.

5 **83 At the end of section 208**

6 Add:

7 *Notifying the Attorney-General*

- 8 (8) The Integrity Commissioner must notify the Attorney-General if
9 the Integrity Commissioner intends to give section 149 certified
10 information to the Inspector-General of Intelligence and Security.

11 ***Ombudsman Act 1976***

12 **84 Subsection 3(1)**

13 Insert:

14 *examiner* of ACC has the meaning given by the *Australian Crime*
15 *Commission Act 2002*.

16 **85 After section 5A**

17 Insert:

18 **5B Transfer of complaints from the Inspector-General of**
19 **Intelligence and Security**

20 A complaint is taken to have been made under this Act in respect
21 of action taken by:

- 22 (a) ACC (except action taken by an examiner of ACC
23 performing functions or exercising powers as an examiner);
24 or
25 (b) the Australian Federal Police;

26 if the Inspector-General of Intelligence and Security transfers all or
27 part of the complaint to the Ombudsman under section 32AD of
28 the *Inspector-General of Intelligence and Security Act 1986*.

Note: A complaint or part of a complaint can also be transferred from the Ombudsman to the Inspector-General of Intelligence and Security under section 6F of this Act.

86 Subsection 6A(1)

After “Ombudsman may”, insert “(subject to subsection (3))”.

87 At the end of section 6A

Add:

- (3) However, the Ombudsman must not, under this section, transfer a complaint or part of a complaint to the Inspector-General of Intelligence and Security.

Note: The Ombudsman may transfer a complaint or part of a complaint made in relation to action taken by ACC to the Inspector-General of Intelligence and Security under section 6F.

88 After section 6E

Insert:

6F Transfer of complaints to the Inspector-General of Intelligence and Security

- (1) This section applies if the Ombudsman forms the opinion that:
- (a) a complainant has complained, or could complain, to the Inspector-General of Intelligence and Security under the *Inspector-General of Intelligence and Security Act 1986* in relation to action taken by:
 - (i) ACC (except action taken by an examiner of ACC performing functions or exercising powers as an examiner); or
 - (ii) the Australian Federal Police; and
 - (b) the complaint could be more appropriately or effectively dealt with by the Inspector-General of Intelligence and Security.

Requirement to consult with Inspector-General of Intelligence and Security

- (2) The Ombudsman:

- 1 (a) must consult the Inspector-General of Intelligence and
2 Security about the complaint or the part of the complaint that
3 relates to the action; and
4 (b) may decide not to investigate the action, or not to continue to
5 investigate the action.

6 *Transfer to Inspector-General of Intelligence and Security*

- 7 (3) If the Ombudsman decides not to investigate, or not to continue to
8 investigate, an action under paragraph (2)(b), and the
9 Inspector-General of Intelligence and Security agrees to the
10 transfer of the complaint or the part of the complaint, the
11 Ombudsman must:
12 (a) transfer the complaint or part to the Inspector-General of
13 Intelligence and Security; and
14 (b) as soon as is reasonably practicable, take reasonable steps to
15 give the complainant written notice that the complaint or part
16 has been transferred; and
17 (c) give the Inspector-General of Intelligence and Security any
18 information or documents relating to the complaint or part
19 that are in the possession, or under the control, of the
20 Ombudsman.

21 *Relationship with other provisions*

- 22 (4) This section does not limit the power of the Ombudsman to
23 transfer a complaint or part of a complaint to the Inspector-General
24 of Intelligence and Security under another provision of this Act or
25 any other Act.
26 (5) Subsection 35(2) does not prevent the Ombudsman, or an officer
27 acting on behalf of the Ombudsman, from giving information or
28 documents under paragraph (3)(c) of this section.

29 **89 At the end of subsection 35(6)**

30 Add:

- 31 ; or (d) from giving information or a document to the
32 Inspector-General of Intelligence and Security in accordance
33 with section 35AB.

1 **90 After section 35AA**

2 Insert:

3 **35AB Disclosure of information and documents to**
4 **Inspector-General of Intelligence and Security**

5 (1) This section applies if:

6 (a) either:

7 (i) the Ombudsman obtains information or a document in
8 relation to a Commonwealth agency (within the
9 meaning of the *Inspector-General of Intelligence and*
10 *Security Act 1986*) in the course of performing a
11 function under this or any other Act; or

12 (ii) the Ombudsman prepares a report or other information
13 in relation to an agency referred to in subparagraph (i);
14 and

15 (b) the Ombudsman is of the opinion that the information,
16 document or report is, or may be, relevant to the performance
17 by the Inspector-General of Intelligence and Security of a
18 function of the Inspector-General.

19 (2) Nothing in this Act precludes the Ombudsman from:

20 (a) disclosing the information; or

21 (b) making a statement that includes the information; or

22 (c) giving the document;

23 to the Inspector-General.

24 **91 At the end of subsections 35B(1) and 35C(1)**

25 Add “, except to the Inspector-General of Intelligence and Security in
26 accordance with section 35AB”.

27 ***Privacy Act 1988***

28 **92 After section 49A**

29 Insert:

1 **49B Transfer of complaints from the Inspector-General of**
2 **Intelligence and Security**

3 An individual is taken to have complained to the Information
4 Commissioner under subsection 36(1) in respect of action taken by
5 ACC or the Australian Federal Police if the Inspector-General of
6 Intelligence and Security transfers all or part of the complaint to
7 the Information Commissioner under section 32AD of the
8 *Inspector-General of Intelligence and Security Act 1986*.

9 **93 Subsection 50(1) (after paragraph (e) of the definition of**
10 ***alternative complaint body*)**

11 Insert:

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

13 **94 After subparagraph 50(2)(a)(iv)**

14 Insert:

15 (iva) to the Inspector-General of Intelligence and Security
16 under the *Inspector-General of Intelligence and Security*
17 *Act 1986*; or

18 **95 After subparagraph 50(3)(a)(iv)**

19 Insert:

20 (iva) to the Inspector-General of Intelligence and Security
21 under the *Inspector-General of Intelligence and Security*
22 *Act 1986*; or

23 ***Public Interest Disclosure Act 2013***

24 **96 Section 8**

25 Insert:

26 ***ACIC*** means the agency known as the Australian Criminal
27 Intelligence Commission established by the *Australian Crime*
28 *Commission Act 2002*.

29 ***examiner*** of ACIC has the meaning given by the *Australian Crime*
30 *Commission Act 2002*.

1 *intelligence function*, in relation to ACIC or the Australian Federal
2 Police, has the meaning given by the *Inspector-General of*
3 *Intelligence and Security Act 1986*.

4 **97 Section 34 (table item 1, column 2, after paragraph (c))**

5 Insert:

6 (ca) if the discloser believes on reasonable grounds that:

7 (i) the disclosure relates to action taken by ACIC or the Australian Federal Police
8 in relation to that agency's intelligence functions; and

9 (ii) it would be appropriate for the disclosure to be investigated by the IGIS;
10 the IGIS;

11 **98 Section 42 (note 2)**

12 After "intelligence agency", insert " , or ACIC or the Australian Federal
13 Police in relation to that agency's intelligence functions".

14 **99 Subparagraph 43(3)(a)(iii)**

15 After "intelligence agency", insert " , or ACIC or the Australian Federal
16 Police in relation to that agency's intelligence functions".

17 **100 After subsection 43(3)**

18 Insert:

19 (3A) The authorised officer must not allocate the handling of the
20 disclosure to the IGIS in relation to action taken by an examiner of
21 ACIC performing functions and exercising powers as an examiner.

22 **101 Paragraphs 44(1A)(a) and (b)**

23 After "intelligence agency", insert " , or ACIC or the Australian Federal
24 Police in relation to that agency's intelligence functions".

25 **102 Section 46 (note)**

26 After "intelligence agency", insert " , or ACIC or the Australian Federal
27 Police in relation to that agency's intelligence functions".

28 **103 At the end of paragraph 50A(1)(b)**

29 Add "and".

104 After paragraph 50A(1)(b)

Insert:

- (c) if the agency is ACIC or the Australian Federal Police—the disclosure does not relate to the intelligence functions of the agency;

105 Paragraph 50A(2)(b)

Repeal the paragraph, substitute:

- (b) either:
 - (i) the agency is an intelligence agency; or
 - (ii) the agency is ACIC or the Australian Federal Police, and the disclosure relates to the intelligence functions of the agency;

106 Subsection 52(4)

Repeal the subsection, substitute:

- (4) If:
 - (a) the agency is the IGIS or an intelligence agency; or
 - (b) the agency is ACIC or the Australian Federal Police, and the disclosure relates to the intelligence functions of the agency; the IGIS may extend, or further extend, the 90-day period by such additional period (which may exceed 90 days) as the IGIS considers appropriate:
 - (c) on the IGIS’s own initiative; or
 - (d) if the agency is not the IGIS—on application made by the principal officer of the agency; or
 - (e) on application made by the discloser.

107 Section 58 (note)

After “intelligence agency”, insert “, or ACIC or the Australian Federal Police in relation to that agency’s intelligence functions”.

108 After paragraph 63(a)

Insert:

- (aa) assisting, in relation to the intelligence functions of ACIC or the Australian Federal Police:
 - (i) principal officers of that agency; and

- (ii) authorised officers of that agency; and
(iii) public officials who belong to that agency; and
(iv) former public officials who belonged to that agency;
in relation to the operation of this Act; and

109 After paragraph 63(b)

Insert:

- (ba) conducting educational and awareness programs relating to this Act, in relation to the intelligence functions of ACIC or the Australian Federal Police, to the extent to which this Act relates to:
(i) that agency; and
(ii) public officials who belong to that agency; and
(iii) former public officials who belonged to that agency;
and

110 Section 63 (note)

Repeal the note, substitute:

- Note: Section 8A of the *Inspector-General of Intelligence and Security Act 1986* extends the IGIS's functions to cover disclosures of information allocated under section 43 of this Act (whether or not they are allocated to the IGIS), if the disclosable conduct with which the information is concerned relates to:
(a) an intelligence agency; or
(b) ACIC or the Australian Federal Police, in relation to the intelligence functions of the agency.

111 Transitional—section 52 of the *Public Interest Disclosure Act 2013*

The amendment of section 52 of the *Public Interest Disclosure Act 2013* made by this Part does not affect the continuity of a period that was extended, or further extended, under subsection 52(4) of that Act before the commencement of this item.

Telecommunications (Interception and Access) Act 1979

112 Subsection 5(1)

Insert:

1 **network activity warrant** has the same meaning as in the
2 *Surveillance Devices Act 2004*.

3 **network activity warrant intercept information** means information
4 obtained under a network activity warrant by intercepting a
5 communication passing over a telecommunications system.

6 **113 Subsection 5(1) (definition of *restricted record*)**

7 Omit “or a record of data disruption intercept information”, substitute “,
8 a record of data disruption intercept information or a record of network
9 activity warrant intercept information”.

10 **114 Subsection 5(1) (paragraph (b) of the definition of**
11 ***warrant*)**

12 After “data disruption warrant”, insert “, a network activity warrant”.

13 **115 Paragraph 7(2)(bb)**

14 Omit “or 27KE(9)”, substitute “, 27KE(9) or 27KP(8)”.

15 **116 After section 63AD**

16 Insert:

17 **63AE Dealing in network activity warrant intercept information etc.**

- 18 (1) A person may, for the purposes of doing a thing authorised by a
19 network activity warrant:
- 20 (a) communicate network activity warrant intercept information
21 to another person; or
- 22 (b) make use of network activity warrant intercept information;
23 or
- 24 (c) make a record of network activity warrant intercept
25 information; or
- 26 (d) give network activity warrant intercept information in
27 evidence in:
- 28 (i) a criminal proceeding for an offence against section 105
29 so far as the offence relates to contravening section 63;
30 or
- 31 (ii) a proceeding that is not a criminal proceeding.

- 1 (2) A person may:
- 2 (a) communicate network activity warrant intercept information
- 3 to another person; or
- 4 (b) make use of network activity warrant intercept information;
- 5 or
- 6 (c) make a record of network activity warrant intercept
- 7 information;
- 8 if the information relates, or appears to relate, to the involvement,
- 9 or likely involvement, of a person in one or more of the following
- 10 activities:
- 11 (d) activities that present a significant risk to a person's safety;
- 12 (e) acting for, or on behalf of, a foreign power (within the
- 13 meaning of the *Australian Security Intelligence Organisation*
- 14 *Act 1979*);
- 15 (f) activities that are, or are likely to be, a threat to security;
- 16 (g) activities that pose a risk, or are likely to pose a risk, to the
- 17 operational security (within the meaning of the *Intelligence*
- 18 *Services Act 2001*) of ASIS (within the meaning of that Act);
- 19 (h) activities that pose a risk, or are likely to pose a risk, to the
- 20 operational security (within the ordinary meaning of that
- 21 expression) of the Organisation or of AGO or ASD (within
- 22 the meanings of the *Intelligence Services Act 2001*);
- 23 (i) activities related to the proliferation of weapons of mass
- 24 destruction or the movement of goods listed from time to
- 25 time in the Defence and Strategic Goods List (within the
- 26 meaning of regulation 13E of the *Customs (Prohibited*
- 27 *Exports) Regulations 1958*);
- 28 (j) activities related to a contravention, or an alleged
- 29 contravention, by a person of a UN sanction enforcement law
- 30 (within the meaning of the *Charter of the United Nations Act*
- 31 *1945*).
- 32 (3) A person may, in connection with:
- 33 (a) the performance by an IGIS official of the IGIS official's
- 34 functions or duties; or
- 35 (b) the exercise by an IGIS official of the IGIS official's powers;
- 36 communicate to the IGIS official, or make use of, or make a record
- 37 of, network activity warrant intercept information.
-

- 1 (4) An IGIS official may, in connection with:
2 (a) the performance by the IGIS official of the IGIS official's
3 functions or duties; or
4 (b) the exercise by the IGIS official of the IGIS official's
5 powers;
6 communicate to another person, or make use of, or make a record
7 of, network activity warrant intercept information.
- 8 (5) If:
9 (a) information was obtained by intercepting a communication
10 passing over a telecommunications system; and
11 (b) the interception was purportedly for the purposes of doing a
12 thing specified in a network activity warrant; and
13 (c) the interception was not authorised by the network activity
14 warrant;
15 then:
16 (d) a person may, in connection with:
17 (i) the performance by an IGIS official of the IGIS
18 official's functions or duties; or
19 (ii) the exercise by an IGIS official of the IGIS official's
20 powers;
21 communicate to the IGIS official, or make use of, or make a
22 record of, that information; and
23 (e) an IGIS official may, in connection with:
24 (i) the performance by the IGIS official of the IGIS
25 official's functions or duties; or
26 (ii) the exercise by the IGIS official of the IGIS official's
27 powers;
28 communicate to another person, or make use of, or make a
29 record of, that information.
- 30 (6) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution
31 for an offence against section 63 of this Act, an IGIS official does
32 not bear an evidential burden in relation to the matters in
33 subsection (4) or (5) of this section.

1 **117 Paragraph 67(1)(a)**

2 Omit “or data disruption intercept information”, substitute “, data
3 disruption intercept information or network activity warrant intercept
4 information”.

5 **118 Section 68**

6 Omit “or data disruption intercept information”, substitute “, data
7 disruption intercept information or network activity warrant intercept
8 information”.

9 **119 Subsection 74(1)**

10 After “data disruption intercept information”, insert “, network activity
11 warrant intercept information”.

12 **120 Subsection 75(1)**

13 After “data disruption warrant”, insert “, a network activity warrant”.

14 **121 Paragraphs 77(1)(a) and (b)**

15 After “63AD,”, insert “63AE,”.

16 **122 After paragraph 108(2)(cc)**

17 Insert:

18 (cd) accessing a stored communication under a network activity
19 warrant; or

Schedule 3—Account takeover warrants

Crimes Act 1914

1 Subsection 3(1) (definition of *law enforcement officer*)

Before “means”, insert “(except in Part IAAC)”.

2 Subsection 3LA(6) (penalty)

Omit “for contravention of this subsection”.

3 At the end of section 3LA

Add:

Additional use of information etc.

- (7) If information or assistance is provided under this section in connection with an investigation into one or more alleged offences, this Act does not, by implication, prevent the information or assistance from being used in connection with the execution of an account takeover warrant (within the meaning of Part IAAC) that relates to that investigation.

4 After Part IAAB

Insert:

Part IAAC—Account takeover warrants

Division 1—Introduction

3ZZUJ Simplified outline of this Part

- An account takeover warrant may be issued by a magistrate.
- An account takeover warrant authorises the Australian Federal Police or the ACC to take control of one or more online accounts.

1
2
3
4
5
6
7
8
9
10

11
12

13
14

15
16
17
18
19

20
21
22
23
24
25
26
27

28
29
30

31
32
33

- The applicant for an account takeover warrant must suspect on reasonable grounds that:
 - (a) one or more relevant offences have been, are being, are about to be, or are likely to be, committed; and
 - (b) an investigation into those offences is being, will be, or is likely to be, conducted; and
 - (c) taking control of the online accounts is necessary, in the course of that investigation, for the purpose of enabling evidence to be obtained of the commission of those offences.
- An emergency authorisation for taking control of an online account may be given by an appropriate authorising officer.
- An emergency authorisation is subject to approval by a magistrate.
- A magistrate may make an order requiring a person to provide any information or assistance that is reasonable and necessary to allow a law enforcement officer to take control of an online account that is the subject of an account takeover warrant or emergency authorisation.
- A person must not use or disclose information that:
 - (a) was obtained under an account takeover warrant or emergency authorisation; or
 - (b) relates to an application for, the issue of, the existence of, or the expiration of, an account takeover warrant or emergency authorisation; or
 - (c) relates to an application for approval of the giving of an emergency authorisation.
- The Australian Federal Police and the ACC must comply with reporting and record keeping requirements relating to account takeover warrants and emergency authorisations.
- The Ombudsman must inspect the records of the Australian Federal Police and the ACC to determine the extent of compliance with this Part by:

- | |
|--|
| <p>(a) the Australian Federal Police and the ACC; and</p> <p>(b) law enforcement officers.</p> |
|--|

Note: This Part confers non-judicial functions and powers on magistrates. Section 4AAA deals with the conferral of non-judicial functions and powers on magistrates.

3ZZUK Definitions

In this Part:

account has the same meaning as in the *Enhancing Online Safety Act 2015*.

account-based data has the same meaning as in Part IAA.

account credentials means information that a user of an online account requires in order to access or operate the account, and includes (for example) each of the following:

- (a) a username;
- (b) a password;
- (c) a PIN;
- (d) a security question or answer;
- (e) a biometric form of identification.

account takeover warrant means a warrant issued under section 3ZZUP or subsection 3ZZVC(2) or (3).

appropriate authorising officer has the meaning given by section 3ZZUM.

carrier means:

- (a) a carrier within the meaning of the *Telecommunications Act 1997*; or
- (b) a carriage service provider within the meaning of that Act.

chief officer means the following:

- (a) in relation to the Australian Federal Police—the Commissioner of the Australian Federal Police;
- (b) in relation to the ACC—the Chief Executive Officer of the ACC.

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

4 **computer** means all or part of:

- 5 (a) one or more computers; or
6 (b) one or more computer systems; or
7 (c) one or more computer networks; or
8 (d) any combination of the above.

9 **electronic service** has the same meaning as in the *Enhancing*
10 *Online Safety Act 2015*.

11 **emergency authorisation** means an emergency authorisation given
12 under section 3ZZUX.

13 **executing officer**, in relation to an account takeover warrant,
14 means:

- 15 (a) the law enforcement officer named in the warrant by the
16 issuing magistrate as being responsible for executing the
17 warrant; or
18 (b) if that law enforcement officer does not intend to execute the
19 warrant—another law enforcement officer whose name has
20 been written in the warrant by the law enforcement officer so
21 named; or
22 (c) another law enforcement officer whose name has been
23 written in the warrant by the law enforcement officer last
24 named in the warrant.

25 **formal application** has the meaning given by
26 paragraph 3ZZUN(2)(a).

27 **IGIS official** means:

- 28 (a) the Inspector-General of Intelligence and Security; or
29 (b) any other person covered by subsection 32(1) of the
30 *Inspector-General of Intelligence and Security Act 1986*.

31 **law enforcement agency** means:

- 32 (a) the Australian Federal Police; or
33 (b) the ACC.

law enforcement officer means the following:

- (a) in relation to the Australian Federal Police:
 - (i) the Commissioner of the Australian Federal Police; or
 - (ii) a Deputy Commissioner of the Australian Federal Police; or
 - (iii) an AFP employee (within the meaning of the *Australian Federal Police Act 1979*); or
 - (iv) a special member of the Australian Federal Police (within the meaning of the *Australian Federal Police Act 1979*); or
 - (v) a person seconded to the Australian Federal Police;
- (b) in relation to the ACC:
 - (i) the Chief Executive Officer of the ACC; or
 - (ii) a member of the staff of the ACC.

Ombudsman official means:

- (a) the Ombudsman; or
- (b) a Deputy Commonwealth Ombudsman; or
- (c) a person who is a member of the staff referred to in subsection 31(1) of the *Ombudsman Act 1976*.

online account means an account that an electronic service has for an end-user.

protected information means:

- (a) any information obtained under an account takeover warrant or an emergency authorisation; or
- (b) information relating to:
 - (i) an application for, the issue of, the existence of, or the expiration of, an account takeover warrant or emergency authorisation; or
 - (ii) an application for approval of the giving of an emergency authorisation.

relevant offence means:

- (a) a serious Commonwealth offence; or
- (b) a serious State offence that has a federal aspect.

1 *serious Commonwealth offence* has the same meaning as in
2 Part IAB.

3 *serious State offence that has a federal aspect* has the same
4 meaning as in Part IAB.

5 *takes control* has the meaning given by section 3ZZUL.

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

8 *urgent application* has the meaning given by
9 paragraph 3ZZUN(2)(b).

10 **3ZZUL When a person takes control of an online account**

11 (1) For the purposes of this Part, a person *takes control* of an online
12 account if the person takes one or more steps that result in the
13 person having exclusive access to the account.

14 (2) The following are examples of such steps:

- 15 (a) using existing account credentials to alter one or more
16 account credentials;
17 (b) removing a requirement for two-factor authentication;
18 (c) altering the kind or kinds of account credentials that are
19 required to access or operate the account.

20 **3ZZUM Appropriate authorising officer**

21 *Australian Federal Police*

22 (1) For the purposes of this Part, an *appropriate authorising officer* of
23 the Australian Federal Police is:

- 24 (a) the chief officer of the Australian Federal Police; or
25 (b) a Deputy Commissioner of the Australian Federal Police; or
26 (c) a senior executive AFP employee who is authorised under
27 subsection (2).

28 (2) The chief officer of the Australian Federal Police may authorise, in
29 writing, a person who is a senior executive AFP employee to be an
30 appropriate authorising officer of the Australian Federal Police for
31 the purposes of this Part.

ACC

- (3) For the purposes of this Part, an *appropriate authorising officer* of the ACC is:
- (a) the chief officer of the ACC; or
 - (b) an executive level member of the staff of the ACC who is authorised under subsection (4).
- (4) The chief officer of the ACC may authorise, in writing, a person who is an executive level member of the staff of the ACC to be an appropriate authorising officer of the ACC for the purposes of this Part.

Division 2—Account takeover warrants

3ZZUMA Sunsetting

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

3ZZUN Application for account takeover warrant

- (1) A law enforcement officer may apply to a magistrate for the issue of an account takeover warrant if the law enforcement officer suspects on reasonable grounds that:
- (a) one or more relevant offences have been, are being, are about to be, or are likely to be, committed; and
 - (b) an investigation into those offences is being, will be, or is likely to be, conducted; and
 - (c) taking control of one or more online accounts (the *target accounts*) is necessary, in the course of that investigation, for the purpose of enabling evidence to be obtained of the commission of those offences.
- (2) An application for an account takeover warrant may be made:
- (a) in person (such an application is a *formal application*); or
 - (b) if the applicant believes that it is impracticable for the application to be made in person—by telephone, email, fax or any other means of communication (such an application is an *urgent application*).
- (2A) An application:

- 1 (a) must specify:
2 (i) the name of the applicant; and
3 (ii) the nature and duration of the warrant sought; and
4 (b) subject to this section, must be supported by an affidavit
5 setting out the grounds on which the warrant is sought.

6 *Unsworn applications*

7 (2B) If a law enforcement officer believes that:

- 8 (a) taking control of the target accounts is immediately
9 necessary, in the course of the investigation mentioned in
10 paragraph (1)(c), for the purpose of enabling evidence to be
11 obtained of the commission of the offences mentioned in that
12 paragraph; and
13 (b) it is impracticable for an affidavit to be prepared or sworn
14 before an application for a warrant is made;

15 an application for an account takeover warrant under subsection (1)
16 may be made before an affidavit is prepared or sworn.

17 (2C) If subsection (2B) applies, the applicant must:

- 18 (a) provide as much information as the magistrate considers is
19 reasonably practicable in the circumstances; and
20 (b) not later than 72 hours after the making of the application,
21 send a duly sworn affidavit to the magistrate, whether or not
22 a warrant has been issued.

23 (2D) If:

- 24 (a) subsection (2B) applies; and
25 (b) transmission by fax is available; and
26 (c) an affidavit has been prepared;

27 the person applying must transmit a copy of the affidavit, whether
28 sworn or unsworn, to the magistrate who is to determine the
29 application.

30 (3) An application (whether formal or urgent) must provide sufficient
31 information to enable the magistrate to decide whether or not to
32 issue the warrant.

- 1 (4) A magistrate may require an applicant to provide such additional
2 information as is necessary for the proper consideration of the
3 application.
- 4 (5) As soon as practicable after making an urgent application that was
5 not made in writing, the applicant must:
6 (a) make a written record of the application; and
7 (b) give a copy of the record to the magistrate to whom the
8 application was made.

9 **3ZZUP Determining the application**

- 10 (1) A magistrate may issue an account takeover warrant if satisfied
11 that there are reasonable grounds for the suspicion founding the
12 application for the warrant.
- 13 (2) In determining whether an account takeover warrant should be
14 issued, the magistrate must have regard to:
15 (a) the nature and gravity of the alleged relevant offence, or
16 alleged relevant offences, in respect of which the warrant is
17 sought; and
18 (b) the existence of any alternative means of obtaining the
19 evidence sought to be obtained; and
20 (c) the extent to which the privacy of any person is likely to be
21 affected; and
22 (d) the likely evidentiary value of any evidence sought to be
23 obtained; and
24 (da) the extent to which the execution of the warrant is likely to
25 impact on persons lawfully using a computer, so far as that
26 matter is known to the magistrate; and
27 (db) the extent to which the execution of the warrant is likely to
28 cause a person to suffer a temporary loss of:
29 (i) money; or
30 (ii) digital currency; or
31 (iii) property (other than data);
32 so far as that matter is known to the magistrate; and
33 (dc) if:
34 (i) the magistrate believes on reasonable grounds that each
35 target account is held by a person who is working in a

- 1 professional capacity as a journalist or of an employer
2 of such a person; and
- 3 (ii) the alleged relevant offence, or each of the alleged
4 relevant offences, in respect of which the warrant is
5 sought is an offence against a secrecy provision;
6 whether the public interest in issuing the warrant outweighs:
- 7 (iii) the public interest in protecting the confidentiality of the
8 identity of the journalist's source; and
- 9 (iv) the public interest in facilitating the exchange of
10 information between journalists and members of the
11 public so as to facilitate reporting of matters in the
12 public interest; and
- 13 (e) any previous warrant sought or issued under this Division in
14 connection with the same online account; and
- 15 (f) any previous warrant sought or issued under this Division in
16 connection with the same alleged relevant offence or the
17 same alleged relevant offences.
- 18 (3) For the purposes of having regard to the nature and gravity of the
19 alleged relevant offence, or alleged relevant offences, in respect of
20 which the warrant is sought, the magistrate must give weight to the
21 following matters:
- 22 (a) whether the conduct constituting the alleged relevant offence,
23 or alleged relevant offences, in respect of which the warrant
24 is sought amounts to:
- 25 (i) an activity against the security of the Commonwealth;
26 or
- 27 (ii) an offence against Chapter 5 of the *Criminal Code*;
- 28 (b) whether the conduct constituting the alleged relevant offence,
29 or alleged relevant offences, in respect of which the warrant
30 is sought amounts to:
- 31 (i) an activity against the proper administration of
32 Government; or
- 33 (ii) an offence against Chapter 7 of the *Criminal Code*;
- 34 (c) whether the conduct constituting the alleged relevant offence,
35 or alleged relevant offences, in respect of which the warrant
36 is sought:
- 37 (i) causes, or has the potential to cause, serious violence, or
38 serious harm, to a person; or
-

-
- 1 (ii) amounts to an offence against Chapter 8 of the *Criminal*
2 *Code*;
- 3 (d) whether the conduct constituting the alleged relevant offence,
4 or alleged relevant offences, in respect of which the warrant
5 is sought:
- 6 (i) causes, or has the potential to cause, a danger to the
7 community; or
- 8 (ii) amounts to an offence against Chapter 9 of the *Criminal*
9 *Code*;
- 10 (e) whether the conduct constituting the alleged relevant offence,
11 or alleged relevant offences, in respect of which the warrant
12 is sought:
- 13 (i) causes, or has the potential to cause, substantial damage
14 to, or loss of, data, property or critical infrastructure; or
- 15 (ii) amounts to an offence against Chapter 10 of the
16 *Criminal Code*;
- 17 (f) whether the conduct constituting the alleged relevant offence,
18 or alleged relevant offences, in respect of which the warrant
19 is sought involves, or is related to, the commission of:
- 20 (i) transnational crime; or
- 21 (ii) serious crime; or
- 22 (iii) organised crime;
- 23 that is not covered by any of the preceding paragraphs.
- 24 (4) Subsection (3) does not limit the matters that may be considered by
25 the magistrate.
- 26 (5) To avoid doubt, this Act does not prevent an account takeover
27 warrant from being issued in a case where the conduct constituting
28 the alleged relevant offence, or alleged relevant offences, in respect
29 of which the warrant is sought is not covered by subsection (3).
- 30 (6) For the purposes of this section, ***secrecy provision*** means a
31 provision of a law of the Commonwealth or of a State that
32 prohibits:
- 33 (a) the communication, divulging or publication of information;
34 or
- 35 (b) the production of, or the publication of the contents of, a
36 document.
-

3ZZUQ What must an account takeover warrant contain?

- (1) An account takeover warrant must:
- (a) state that the magistrate issuing the warrant is satisfied of the matters referred to in subsection 3ZZUP(1) and has had regard to the matters referred to in subsection 3ZZUP(2); and
 - (b) specify:
 - (i) the name of the applicant; and
 - (ii) the name of the law enforcement officer who, unless the officer inserts the name of another law enforcement officer in the warrant, is to be responsible for executing the warrant; and
 - (iii) the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is issued; and
 - (iv) the date the warrant is issued; and
 - (v) the period during which the warrant is in force (see subsection (3)); and
 - (vi) each target account; and
 - (vii) for each target account where the holder of the target account is known to the applicant—the holder; and
 - (viii) for each target account where one or more users of the target account (other than the holder of the target account) are known to the applicant—those users; and
 - (ix) any conditions subject to which things may be done under the warrant; and
 - (c) set out an outline of the investigation to which the warrant relates.
- (2) For the purposes of subparagraph (1)(b)(vi), a target account may be specified by identifying one or more matters or things that are sufficient to identify the target account.
- (3) A warrant may only be issued for a period of no more than 90 days.
- Note: The execution of a warrant may be discontinued earlier—see section 3ZZUU.
- (4) A warrant must be signed by the person issuing it and include the person's name.

3ZZUR What an account takeover warrant authorises

- (1) An account takeover warrant must authorise the doing of specified things (subject to any restrictions or conditions specified in the warrant) in relation to each target account.
- (2) The things that may be specified are any of the following that the magistrate considers appropriate in the circumstances:
 - (a) taking control of the target account at any time while the warrant is in force, if doing so is necessary, in the course of the investigation to which the warrant relates, for the purpose of enabling evidence to be obtained of the commission of the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is issued;
 - (b) using:
 - (i) a computer; or
 - (ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or
 - (iii) any other electronic equipment; or
 - (iv) a data storage device;for the purpose of taking control of the target account as mentioned in paragraph (a);
 - (c) if necessary for the purpose of taking control of the target account as mentioned in paragraph (a):
 - (i) accessing account-based data to which the target account relates; or
 - (ii) adding, copying, deleting or altering account credentials to which the target account relates; or
 - (iii) adding, copying, deleting or altering data in a computer;
 - (d) if, having regard to other methods (if any) of taking control of the target account which are likely to be as effective, it is reasonable in all the circumstances to do so:
 - (i) using a communication in transit for the purpose of taking control of the target account as mentioned in paragraph (a); and
 - (ii) if necessary to achieve that purpose—adding, copying, deleting or altering data in the communication in transit;
 - (e) copying any account-based data to which the target account relates, and that:

- 1 (i) appears to be relevant for the purposes of determining
2 whether the account-based data is covered by the
3 warrant; or
4 (ii) is covered by the warrant;
5 (f) copying any account credentials to which the target account
6 relates;
7 (g) any other thing reasonably incidental to any of the above.

- 8 (3) For the purposes of paragraph (2)(e), if:
9 (a) access has been obtained to account-based data; and
10 (b) the account-based data is subject to a form of electronic
11 protection;
12 the account-based data is taken to be relevant for the purposes of
13 determining whether the account-based data is covered by the
14 warrant.

15 *When account-based data is covered by a warrant*

- 16 (4) For the purposes of this section, account-based data is **covered by** a
17 warrant if access to the data is necessary, in the course of the
18 investigation to which the warrant relates, for the purpose of
19 enabling evidence to be obtained of the commission of the alleged
20 relevant offence, or alleged relevant offences, in respect of which
21 the warrant is issued.

22 *Certain acts not authorised*

- 23 (5) Subsection (2) does not authorise the addition, deletion or
24 alteration of data, or the doing of any thing, that is likely to:
25 (a) materially interfere with, interrupt or obstruct:
26 (i) a communication in transit; or
27 (ii) the lawful use by other persons of a computer;
28 unless the addition, deletion or alteration, or the doing of the
29 thing, is necessary to do one or more of the things specified
30 in the warrant; or
31 (b) cause any other material loss or damage to other persons
32 lawfully using a computer.

Concealment of access etc.

- (6) If any thing has been done under:
- (a) an account takeover warrant; or
 - (b) this subsection;
- then, in addition to the things specified in the warrant, the warrant authorises the doing of any of the following:
- (c) any thing reasonably necessary to conceal the fact that any thing has been done under the warrant or under this subsection;
 - (d) if, having regard to other methods (if any) of doing the things mentioned in paragraph (c) which are likely to be as effective, it is reasonable in all the circumstances to do so:
 - (i) using a computer or a communication in transit to do those things; and
 - (ii) if necessary to achieve that purpose—adding, copying, deleting or altering other data in the computer or the communication in transit;
 - (e) any other thing reasonably incidental to any of the above;
- at the following time:
- (f) at any time while the warrant is in force or within 28 days after it ceases to be in force;
 - (g) if none of the things mentioned in paragraph (c) are done within the 28-day period mentioned in paragraph (f)—at the earliest time after that 28-day period at which it is reasonably practicable to do the things mentioned in paragraph (c).
- (7) Subsection (6) does not authorise the doing of a thing that is likely to:
- (a) materially interfere with, interrupt or obstruct:
 - (i) a communication in transit; or
 - (ii) the lawful use by other persons of a computer;
 unless the doing of the thing is necessary to do one or more of the things specified in subsection (6); or
 - (b) cause any other material loss or damage to other persons lawfully using a computer.

Statutory conditions

- (8) An account takeover warrant is subject to the following conditions:
- (a) the warrant must not be executed in a manner that results in loss or damage to data unless the damage is justified and proportionate, having regard to the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is issued;
 - (b) the warrant must not be executed in a manner that causes a person to suffer a permanent loss of:
 - (i) money; or
 - (ii) digital currency; or
 - (iii) property (other than data).
- (9) Subsection (8) does not, by implication, limit the conditions to which an account takeover warrant may be subject.
- (10) The conditions set out in subsection (8) must be specified in an account takeover warrant.

3ZZUS Variation of account takeover warrant

- (1) A law enforcement officer to whom an account takeover warrant has been issued may, by writing, apply at any time before the expiry of the warrant:
- (a) for an extension of the warrant for a period of no more than 90 days after the day the warrant would otherwise expire; or
 - (b) for a variation of any of the other terms of the warrant.
- (2) The application is to be made to a magistrate and must be accompanied by the original warrant.
- (3) The magistrate may, by writing, grant an application if satisfied that the matters referred to in subsection 3ZZUP(1) still exist, having regard to the matters in subsection 3ZZUP(2).
- (4) If the magistrate grants the application, the magistrate must endorse the new expiry date or the other varied term on the original warrant.
- (5) An application may be made under this section more than once.

3ZZUT Revocation of account takeover warrant

- (1) If an account takeover warrant is in force, a magistrate may, by instrument in writing, revoke the warrant.
- (2) If the circumstances set out in subsection 3ZZUU(2) apply in relation to an account takeover warrant:
 - (a) if the warrant was issued in response to an application made by a law enforcement officer of the Australian Federal Police—the chief officer of the Australian Federal Police must, by instrument in writing, revoke the warrant; or
 - (b) if the warrant was issued in response to an application made by a law enforcement officer of the Australian Crime Commission—the chief officer of the Australian Crime Commission must, by instrument in writing, revoke the warrant.
- (3) The instrument revoking a warrant must be signed by the magistrate or the chief officer, as the case requires.
- (4) If a magistrate revokes an account takeover warrant, the magistrate must give a copy of the instrument of revocation to:
 - (a) if the warrant was issued in response to an application made by a law enforcement officer of the Australian Federal Police—the chief officer of the Australian Federal Police; or
 - (b) if the warrant was issued in response to an application made by a law enforcement officer of the ACC—the chief officer of the ACC.
- (5) If:
 - (a) a magistrate revokes an account takeover warrant; and
 - (b) at the time of the revocation, a law enforcement officer is executing the warrant;the law enforcement officer is not subject to any civil or criminal liability for any act done in the proper execution of that warrant before the officer is made aware of the revocation.

3ZZUU Discontinuance of execution of account takeover warrant

Scope

- (1) This section applies if an account takeover warrant is issued.

Discontinuance of execution of account takeover warrant

- (2) If:

(a) the warrant was sought by a law enforcement officer of the Australian Federal Police or the Australian Crime Commission; and

(b) the chief officer is satisfied that taking control of the target account is no longer required for the purpose of enabling evidence to be obtained of the commission of the alleged relevant offence, or any of the alleged relevant offences, in respect of which the warrant is issued;

the chief officer must, in addition to revoking the warrant under section 3ZZUT, take the steps necessary to ensure that the execution of the warrant is discontinued.

- (3) If:

(a) the warrant was sought by a law enforcement officer of the Australian Federal Police or the Australian Crime Commission; and

(b) the chief officer is notified that the warrant has been revoked by a magistrate under section 3ZZUT;

the chief officer must take the steps necessary to ensure that the execution of the warrant is discontinued as soon as practicable.

- (4) If the executing officer believes that taking control of the target account is no longer required for the purpose of enabling evidence to be obtained of the commission of the alleged relevant offence, or any of the alleged relevant offences, in respect of which the warrant is issued, the executing officer must immediately inform the chief officer of the law enforcement agency to which the executing officer belongs or is seconded.

3ZZUV Restoration of online account

If:

-
- (a) an account takeover warrant ceases to be in force; and
 - (b) it is lawful for the holder of a target account to operate the account; and
 - (c) as a result of the execution of the warrant, the holder of the account cannot operate the account;
- the executing officer must take all reasonable steps to ensure the holder of the account is able to operate the account.

3ZZUW Relationship of this Division to parliamentary privileges and immunities

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

- (a) each House of the Parliament;
- (b) the members of each House of the Parliament;
- (c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

Division 3—Emergency authorisations

3ZZUWA Sunsetting

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

3ZZUX Emergency authorisation—serious risks to person or property

- (1) A law enforcement officer may apply to an appropriate authorising officer for an emergency authorisation for taking control of an online account if, in the course of an investigation of one or more relevant offences, the law enforcement officer reasonably suspects that:
 - (a) an imminent risk of serious violence to a person or substantial damage to property exists; and
 - (b) taking control of the account is immediately necessary for the purpose of dealing with that risk; and
 - (c) the circumstances are so serious and the matter is of such urgency that taking control of the account is warranted; and

- 1 (d) it is not practicable in the circumstances to apply for an
2 account takeover warrant.
- 3 (2) The application may be made orally, in writing or by telephone,
4 fax, email or any other means of communication.
- 5 (3) The appropriate authorising officer may give the emergency
6 authorisation if satisfied that there are reasonable grounds for the
7 suspicion founding the application.

8 *Statutory conditions*

- 9 (4) An emergency authorisation is subject to the following conditions:
- 10 (a) the authorisation must not be executed in a manner that
11 results in damage to data unless the damage is justified and
12 proportionate, having regard to the risk of serious violence or
13 substantial damage referred to in paragraph (1)(a);
- 14 (b) the authorisation must not be executed in a manner that
15 causes a person to suffer a permanent loss of:
- 16 (i) money; or
17 (ii) digital currency; or
18 (iii) property (other than data).

19 **3ZZUY Record of emergency authorisations to be made**

- 20 As soon as practicable after an appropriate authorising officer
21 gives an emergency authorisation, the officer must make a written
22 record of the giving of that authorisation, including in the record:
- 23 (a) the name of the applicant for the authorisation; and
24 (b) the date and time the authorisation was given; and
25 (c) the nature of the authorisation given.

26 **3ZZUZ Attributes of emergency authorisations**

- 27 (1) An emergency authorisation may authorise anything that an
28 account takeover warrant may authorise.
- 29 (2) A law enforcement officer may take control of an online account
30 under an emergency authorisation only if the officer is acting in the
31 performance of the officer's duty.

3ZZVA Application for approval of emergency authorisation

- (1) Within 48 hours after giving an emergency authorisation to a law enforcement officer, the appropriate authorising officer who gave the authorisation (or another person on that appropriate authorising officer's behalf) must apply to a magistrate for approval of the giving of the emergency authorisation.
- (2) The application must:
 - (a) provide sufficient information to enable the magistrate to decide whether or not to approve the giving of the emergency authorisation; and
 - (b) be accompanied by a copy of the written record made under section 3ZZUY in relation to the emergency authorisation.

3ZZVB Consideration of application

- Before deciding an application for approval of the giving of an emergency authorisation that relates to an online account, the magistrate considering the application must, in particular, and being mindful of the intrusive nature of taking control of the online account, consider the following:
- (a) the nature of the risk of serious violence to a person or substantial damage to property;
 - (b) the extent to which issuing an account takeover warrant would have helped reduce or avoid the risk;
 - (c) the extent to which law enforcement officers could have used alternative methods of investigation to help reduce or avoid the risk;
 - (d) how much the use of alternative methods of investigation could have helped reduce or avoid the risk;
 - (e) how much the use of alternative methods of investigation would have prejudiced the safety of the person or property because of delay or for another reason;
 - (f) whether or not it was practicable in the circumstances to apply for an account takeover warrant.

3ZZVC Magistrate may approve giving of an emergency authorisation

- (1) After considering an application for approval of the giving of an emergency authorisation that relates to an online account, the magistrate may give the approval if satisfied that there were reasonable grounds to suspect that:
 - (a) there was a risk of serious violence to a person or substantial damage to property; and
 - (b) taking control of the online account may have helped reduce the risk; and
 - (c) it was not practicable in the circumstances to apply for an account takeover warrant.
- (2) If the magistrate approves the giving of an emergency authorisation, the magistrate may:
 - (a) unless paragraph (b) applies—issue an account takeover warrant relating to taking control of the online account as if the application for the approval were an application for an account takeover warrant under Division 2; or
 - (b) if the magistrate is satisfied that, since the application for the emergency authorisation, the activity that required taking control of an online account has ceased—order the cessation of taking control of the online account.
- (3) If the magistrate does not approve the giving of an emergency authorisation, the magistrate may:
 - (a) order the cessation of taking control of the online account; or
 - (b) if the magistrate is of the view that, although the situation did not warrant the emergency authorisation at the time when the authorisation was given, the use of an account takeover warrant under Division 2 is currently justified—issue an account takeover warrant relating to the taking control of the online account as if the application for the approval were an application for an account takeover warrant under Division 2.
- (4) In any case, the magistrate may order that any information obtained from or relating to the exercise of powers under the emergency authorisation, or any record of that information, be dealt with in a manner specified in the order, so long as the manner does not involve the destruction of that information.

3ZZVD Admissibility of evidence

If the giving of an emergency authorisation is approved under section 3ZZVC, any evidence obtained because of the exercise of powers under that authorisation is not inadmissible in any proceeding only because the evidence was obtained before the approval.

3ZZVE Restoration of online account

If:

- (a) a magistrate orders the cessation of taking control of the online account to which an emergency authorisation relates; and
 - (b) as a result of the execution of the authorisation, the holder of the account cannot operate the account;
- the law enforcement officer who applied for the authorisation must take all reasonable steps to ensure the holder of the account is able to operate the account.

3ZZVF Relationship of this Division to parliamentary privileges and immunities

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

- (a) each House of the Parliament;
- (b) the members of each House of the Parliament;
- (c) the committees of each House of the Parliament and joint committees of both Houses of the Parliament.

Division 4—Assistance orders

3ZZVG Person with knowledge of an online account to provide assistance

- (1) If an account takeover warrant or emergency authorisation is in force, a law enforcement officer may apply to a magistrate for an order (the *assistance order*) requiring a specified person to provide any information or assistance that is reasonable and necessary to

1 allow the law enforcement officer to take control of an online
2 account that is the subject of the warrant or authorisation.

3 *Grant of assistance order*

4 (2) The magistrate may grant the assistance order if the magistrate is
5 satisfied that:

6 (a) there are reasonable grounds for suspecting that taking
7 control of the account is necessary, in the course of the
8 investigation to which the account takeover warrant relates,
9 for the purpose of enabling evidence to be obtained of the
10 commission of the alleged relevant offence, or any of the
11 alleged relevant offences, in respect of which the warrant is
12 issued; and

13 (b) the specified person is:

14 (i) reasonably suspected of having committed the alleged
15 relevant offence, or any of the alleged relevant offences,
16 in respect of which the warrant is issued; or

17 (ii) the holder of the account; or

18 (iii) an employee of the holder of the account; or

19 (iv) a person engaged under a contract for services by the
20 holder of the account; or

21 (v) a person who uses or has used the account; or

22 (vi) a person who is or was a system administrator for the
23 electronic service to which the account relates; and

24 (c) the specified person has relevant knowledge of:

25 (i) the account; or

26 (ii) the electronic service to which the account relates; or

27 (iii) measures applied to protect account-based data to which
28 the account relates.

29 (2A) In determining whether the assistance order should be granted, the
30 magistrate must have regard to whether the specified person is, or
31 has been, subject to:

32 (a) another order under this section; or

33 (b) an order under section 3LA of this Act; or

34 (c) an order under section 64A or 64B of the *Surveillance*
35 *Devices Act 2004*;

36 so far as that matter is known to the magistrate.

1 (2B) Subsection (2B) does not limit the matters to which the magistrate
2 may have regard.

3 *Duration of assistance order*

4 (2C) If an assistance order is granted in relation to a computer that is the
5 subject of an account takeover warrant, the order ceases to be in
6 force when the warrant ceases to be in force.

7 (2D) If an assistance order is granted in relation to a computer that is the
8 subject of an emergency authorisation, the order ceases to be in
9 force when the emergency authorisation ceases to be in force.

10 *Protection from civil liability*

11 (2E) A person is not subject to any civil liability in respect of an act
12 done by the person:

- 13 (a) in compliance with an assistance order; or
- 14 (b) in good faith in purported compliance with an assistance
15 order.

16 *Offence*

- 17 (3) A person commits an offence if:
 - 18 (a) the person is subject to an order under this section; and
 - 19 (b) the person is capable of complying with a requirement in the
20 order; and
 - 21 (c) the person omits to do an act; and
 - 22 (d) the omission contravenes the requirement.

23 Penalty: Imprisonment for 10 years or 600 penalty units, or both.

24 *Additional use of information etc.*

- 25 (4) If information or assistance is provided under this section in
26 connection with an investigation into one or more alleged relevant
27 offences, this Act does not, by implication, prevent the information
28 or assistance from being used in connection with the execution of a
29 section 3E warrant that relates to that investigation.

Division 5—Restrictions on use and disclosure of information

3ZZVH Unauthorised use or disclosure of protected information

- (1) A person commits an offence if:
- (a) the person uses or discloses information; and
 - (b) the information is protected information.

Penalty: Imprisonment for 2 years.

- (2) A person commits an offence if:
- (a) the person uses or discloses any information; and
 - (b) the information is protected information; and
 - (c) the use or disclosure of the information endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence.

Penalty: Imprisonment for 10 years.

Exceptions

- (3) Subsections (1) and (2) do not apply if the use or disclosure was:
- (a) in connection with the administration or execution of this Part; or
 - (b) in connection with the functions of the Australian Federal Police under section 8 of the *Australian Federal Police Act 1979*; or
 - (c) in connection with the functions of the ACC under section 7A of the *Australian Crime Commission Act 2002*; or
 - (d) in connection with preventing, investigating or prosecuting an offence; or
 - (e) by a person who believes on reasonable grounds that the use or disclosure is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property; or
 - (f) for the purposes of any legal proceedings arising out of or otherwise related to this Part or of any report of any such proceedings; or

- 1 (g) for the purposes of obtaining legal advice in relation to this
2 Part; or
- 3 (h) in accordance with any requirement imposed by law; or
- 4 (i) in connection with the performance of functions or duties, or
5 the exercise of powers, under this Part; or
- 6 (j) in connection with the performance of functions or duties, or
7 the exercise of powers, by:
 - 8 (i) a law enforcement officer; or
 - 9 (ii) the Director-General (within the meaning of the
10 *Australian Security Intelligence Organisation Act*
11 *1979*), an ASIO employee (within the meaning of that
12 Act) or an ASIO affiliate (within the meaning of that
13 Act); or
 - 14 (iii) the agency head (within the meaning of the *Intelligence*
15 *Services Act 2001*), or a staff member (within the
16 meaning of that Act), of an agency (within the meaning
17 of that Act); or
- 18 (k) for the purposes of the admission of evidence in a proceeding
19 that is not a criminal proceeding.

20 Note: A defendant bears an evidential burden in relation to the matters in
21 this subsection—see subsection 13.3(3) of the *Criminal Code*.

- 22 (4) Subsections (1) and (2) do not apply if the disclosure was made by
23 a person to an Ombudsman official (whether in connection with a
24 complaint made to the Ombudsman or in any other circumstances).

25 Note: A defendant bears an evidential burden in relation to the matters in
26 this subsection—see subsection 13.3(3) of the *Criminal Code*.

- 27 (5) Subsections (1) and (2) do not apply if the disclosure was made by
28 a person to an IGIS official for the purposes of the IGIS official
29 exercising powers, or performing functions or duties, as an IGIS
30 official.

31 Note: A defendant bears an evidential burden in relation to the matters in
32 this subsection—see subsection 13.3(3) of the *Criminal Code*.

33 **3ZZVJ Dealing with records obtained under, or relating to, account** 34 **takeover warrants etc.**

35 The chief officer of the Australian Federal Police or the ACC:

- 1 (a) must ensure that every record or report comprising protected
2 information is kept in a secure place that is not accessible to
3 people who are not entitled to deal with the record or report;
4 and
5 (b) must cause to be destroyed any record or report referred to in
6 paragraph (a):
7 (i) as soon as practicable after the making of the record or
8 report if the chief officer is satisfied that no civil or
9 criminal proceeding to which the material contained in
10 the record or report relates has been, or is likely to be,
11 commenced and that the material contained in the
12 record or report is not likely to be required in
13 connection with an activity or purpose referred to in
14 subsection 3ZZVH(2), (3) or (4); and
15 (ii) within the period of 5 years after the making of the
16 record or report, and within each period of 5 years
17 thereafter, unless, before the end of that period, the chief
18 officer is satisfied in relation to the material contained
19 in the record or report of a matter referred to in
20 subparagraph (i) and certifies to that effect.

21 **3ZZVK Protection of account takeover technologies and methods**

- 22 (1) In a proceeding, a person may object to the disclosure of
23 information on the ground that the information, if disclosed, could
24 reasonably be expected to reveal details of account takeover
25 technologies or methods.
26 (2) If the person conducting or presiding over the proceeding is
27 satisfied that the ground of objection is made out, the person may
28 order that the person who has the information not be required to
29 disclose it in the proceeding.
30 (3) In determining whether or not to make an order under
31 subsection (2), the person conducting or presiding over the
32 proceeding must take into account whether disclosure of the
33 information:
34 (a) is necessary for the fair trial of the defendant; or
35 (b) is in the public interest.

-
- 1 (4) Subsection (2) does not affect a provision of another law under
2 which a law enforcement officer cannot be compelled to disclose
3 information or make statements in relation to the information.
- 4 (5) If the person conducting or presiding over a proceeding is satisfied
5 that publication of any information disclosed in the proceeding
6 could reasonably be expected to reveal details of account takeover
7 technologies or methods, the person must make any orders
8 prohibiting or restricting publication of the information that the
9 person considers necessary to ensure that those details are not
10 revealed.
- 11 (6) Subsection (5) does not apply to the extent that the person
12 conducting or presiding over the proceeding considers that the
13 interests of justice require otherwise.
- 14 (7) In this section:
- 15 ***account takeover technologies or methods*** means:
- 16 (a) technologies or methods relating to the use of:
- 17 (i) a computer; or
- 18 (ii) a telecommunications facility operated or provided by
19 the Commonwealth or a carrier; or
- 20 (iii) any other electronic equipment; or
- 21 (iv) a data storage device;
- 22 for the purpose of taking control of an online account; or
- 23 (b) technologies or methods relating to adding, copying, deleting
24 or altering account-based data, if doing so is necessary to
25 achieve the purpose mentioned in paragraph (a); or
- 26 (c) technologies or methods relating to adding, copying, deleting
27 or altering account credentials to which an online account
28 relates, if doing so is necessary to achieve the purpose
29 mentioned in paragraph (a);
- 30 where the technologies or methods have been, or are being,
31 deployed in giving effect to an account takeover warrant or
32 emergency authorisation.
- 33 ***proceeding*** includes a proceeding before a court, tribunal or Royal
34 Commission.
-

Division 6—Reporting and record keeping

3ZZVL Chief officers' annual reports to the Minister and the Ombudsman

- (1) As soon as practicable after 30 June in each year, the chief officer of the Australian Federal Police or the ACC must submit a report to the Minister and the Ombudsman that sets out:
- (a) the number of applications for account takeover warrants made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires, during the previous 12 months, and the dates on which those applications were made; and
 - (b) the number of account takeover warrants issued during the previous 12 months in response to applications made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires, and the dates on which those warrants were issued; and
 - (c) if one or more applications for account takeover warrants made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires, during the previous 12 months were refused:
 - (i) the number of those refusals; and
 - (ii) the dates on which those refusals occurred; and
 - (d) if one or more applications for variations of account takeover warrants were made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires, during the previous 12 months:
 - (i) the number of those applications; and
 - (ii) the dates on which those applications were made; and
 - (e) if one or more variations of account takeover warrants were made during the previous 12 months in response to applications made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires:
 - (i) the number of those variations; and
 - (ii) the dates on which those variations were made; and
 - (f) if one or more applications for variations of account takeover warrants made by law enforcement officers of the Australian

Federal Police or the ACC, as the case requires, during the previous 12 months were refused:

- (i) the number of those refusals; and
- (ii) the dates on which those refusals occurred; and
- (g) if one or more account takeover warrants issued in response to applications made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires, were revoked during the previous 12 months:
 - (i) the number of those revocations; and
 - (ii) the dates on which those revocations occurred; and
- (h) for each account takeover warrant that:
 - (i) was issued in response to an application made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires; and
 - (ii) ceased to be in force during the previous 12 months; the following information:
 - (iii) the date the warrant ceased to be in force;
 - (iv) whether the warrant expired or was revoked;
 - (v) whether or not the warrant was executed;
 - (vi) if the warrant was executed—the information listed in subsection (2);
 - (vii) if the warrant was not executed—the reason why the warrant was not executed; and
 - (i) the number of applications for emergency authorisations made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires, during the previous 12 months, and the dates on which those applications were made; and
 - (j) the number of emergency authorisations given during the previous 12 months in response to applications made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires, and the dates on which those authorisations were given; and
 - (k) if one or more applications for emergency authorisations made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires, during the previous 12 months were refused:
 - (i) the number of those refusals; and

- 1 (ii) the dates on which those refusals occurred; and
- 2 (l) if one or more applications for approval of the giving of
- 3 emergency authorisations were made by or on behalf of
- 4 appropriate authorising officers of the Australian Federal
- 5 Police or the ACC, as the case requires, during the previous
- 6 12 months:
- 7 (i) the number of those applications; and
- 8 (ii) the dates on which those applications were made; and
- 9 (m) if the giving of one or more emergency authorisations were
- 10 approved during the previous 12 months in response to
- 11 applications made by or on behalf of appropriate authorising
- 12 officers of the Australian Federal Police or the ACC, as the
- 13 case requires:
- 14 (i) the number of those approvals; and
- 15 (ii) the dates on which those approvals were given; and
- 16 (n) if one or more applications for approval of the giving of
- 17 emergency authorisations made by or on behalf of
- 18 appropriate authorising officers of the Australian Federal
- 19 Police or the ACC, as the case requires, during the previous
- 20 12 months were refused:
- 21 (i) the number of those refusals; and
- 22 (ii) the dates on which those refusals occurred.
- 23 (2) The following information is listed for the purposes of
- 24 subparagraph (1)(h)(vi):
- 25 (a) the name of the executing officer;
- 26 (b) the names of any other law enforcement officers involved in
- 27 executing the warrant;
- 28 (c) the period during which the warrant was executed;
- 29 (d) the target account;
- 30 (e) if the holder of the target account is known to the executing
- 31 officer—the holder;
- 32 (f) if one or more users of the target account (other than the
- 33 holder of the target account) are known to the executing
- 34 officer—those users;
- 35 (g) details of the benefit of the execution of the warrant to the
- 36 investigation of a relevant offence;
-

-
- 1 (h) details of how information obtained under the warrant was
2 used;
3 (i) details of the communication of information obtained under
4 the warrant to persons other than:
5 (i) if the warrant was issued in response to an application
6 made by a law enforcement officer of the Australian
7 Federal Police—law enforcement officers of the
8 Australian Federal Police; or
9 (ii) if the warrant was issued in response to an application
10 made by a law enforcement officer of the ACC—law
11 enforcement officers of the ACC;
12 (j) details of the compliance with the conditions (if any) to
13 which the warrant was subject.
14 (3) For the purposes of paragraph (2)(d), the target account may be
15 specified by identifying one or more matters and things that are
16 sufficient to identify the account.

17 **3ZZVM Chief officers’ annual reports to the Minister**

- 18 (1) As soon as practicable, and in any event within 3 months, after the
19 end of each financial year, the chief officer of the Australian
20 Federal Police or the ACC must submit a report to the Minister that
21 sets out:
22 (a) the number of applications for account takeover warrants
23 made by law enforcement officers of the Australian Federal
24 Police or the ACC, as the case requires, during the financial
25 year; and
26 (b) the number of account takeover warrants issued during the
27 financial year in response to applications made by law
28 enforcement officers of the Australian Federal Police or the
29 ACC, as the case requires; and
30 (c) if one or more applications for account takeover warrants
31 made by law enforcement officers of the Australian Federal
32 Police or the ACC, as the case requires, during the financial
33 year were refused—the number of those refusals; and
34 (d) the number of urgent applications for account takeover
35 warrants made by law enforcement officers of the Australian
36 Federal Police or the ACC, as the case requires, during the
37 financial year; and
-

- 1 (e) the number of account takeover warrants issued during the
2 financial year in response to urgent applications made by law
3 enforcement officers of the Australian Federal Police or the
4 ACC, as the case requires; and
- 5 (f) if one or more urgent applications for account takeover
6 warrants made by law enforcement officers of the Australian
7 Federal Police or the ACC, as the case requires, during the
8 financial year were refused—the number of those refusals;
9 and
- 10 (g) if one or more variations of account takeover warrants were
11 granted during the financial year in response to applications
12 made by law enforcement officers of the Australian Federal
13 Police or the ACC, as the case requires—the number of those
14 variations; and
- 15 (h) if one or more applications for variations of account takeover
16 warrants made by law enforcement officers of the Australian
17 Federal Police or the ACC, as the case requires, during the
18 financial year were refused—the number of those refusals;
19 and
- 20 (i) the number of applications for emergency authorisations
21 made by law enforcement officers of the Australian Federal
22 Police or the ACC, as the case requires, during the financial
23 year; and
- 24 (j) the number of emergency authorisations given during the
25 financial year in response to applications made by law
26 enforcement officers of the Australian Federal Police or the
27 ACC, as the case requires; and
- 28 (k) if one or more applications for emergency authorisations
29 made by law enforcement officers of the Australian Federal
30 Police or the ACC, as the case requires, during the financial
31 year were refused—the number of those refusals; and
- 32 (l) if one or more applications for approval of the giving of
33 emergency authorisations were made by or on behalf of
34 appropriate authorising officers of the Australian Federal
35 Police or the ACC, as the case requires, during the financial
36 year—the number of those applications; and
- 37 (m) if the giving of one or more emergency authorisations were
38 approved during the financial year in response to applications
39 made by or on behalf of appropriate authorising officers of

-
- 1 the Australian Federal Police or the ACC, as the case
 2 requires—the number of those approvals; and
- 3 (n) if one or more applications for approval of the giving of
 4 emergency authorisations made by or on behalf of
 5 appropriate authorising officers of the Australian Federal
 6 Police or the ACC, as the case requires, during the financial
 7 year were refused—the number of those refusals; and
- 8 (o) the types of relevant offences in respect of which account
 9 takeover warrants or emergency authorisations were sought
 10 by law enforcement officers of the Australian Federal Police
 11 or the ACC, as the case requires, during the financial year;
 12 and
- 13 (p) the number of arrests that were made during the financial
 14 year on the basis (wholly or partly) of information obtained
 15 under account takeover warrants issued, or emergency
 16 authorisations given, in response to applications made by law
 17 enforcement officers of the Australian Federal Police or the
 18 ACC, as the case requires; and
- 19 (q) the number of prosecutions for relevant offences that were
 20 commenced during the financial year in which information
 21 obtained under account takeover warrants or emergency
 22 authorisations was given in evidence, and the number of
 23 those prosecutions in which a person was found guilty.
- 24 (2) The Minister must cause a copy of the report to be tabled in each
 25 House of the Parliament within 15 sitting days of that House after
 26 the Minister receives it.
- 27 (3) A copy of a report given to the Minister under this section must be
 28 given to the Ombudsman at the same time as it is given to the
 29 Minister.

30 **3ZZVN Keeping documents connected with account takeover**
 31 **warrants**

- 32 The chief officer of the Australian Federal Police or the ACC must
 33 cause the following to be kept:
- 34 (a) a copy of each application for an account takeover warrant
 35 that was made by a law enforcement officer of the Australian
 36 Federal Police or the ACC, as the case requires;
-

- 1 (b) a copy of each account takeover warrant that was issued in
- 2 response to an application made by a law enforcement officer
- 3 of the Australian Federal Police or the ACC, as the case
- 4 requires;
- 5 (c) each written application for an emergency authorisation made
- 6 by a law enforcement officer of the Australian Federal Police
- 7 or the ACC, as the case requires;
- 8 (d) a copy of each emergency authorisation that was given in
- 9 response to an application made by a law enforcement officer
- 10 of the Australian Federal Police or the ACC, as the case
- 11 requires;
- 12 (e) a copy of each application made by or on behalf of an
- 13 appropriate authorising officer for approval of the giving of
- 14 an emergency authorisation to a law enforcement officer of
- 15 the Australian Federal Police or the ACC, as the case
- 16 requires;
- 17 (f) a copy of each section 3ZZVG assistance order that was
- 18 made in response to an application made by a law
- 19 enforcement officer of the Australian Federal Police or the
- 20 ACC, as the case requires;
- 21 (g) a copy of each application for a section 3ZZVG assistance
- 22 order that was made by a law enforcement officer of the
- 23 Australian Federal Police or the ACC, as the case requires;
- 24 (h) if an application for a variation of an account takeover
- 25 warrant was made by a law enforcement officer of the
- 26 Australian Federal Police or the ACC, as the case requires—a
- 27 copy of the application;
- 28 (i) if an account takeover warrant that was varied in response to
- 29 an application made by a law enforcement officer of the
- 30 Australian Federal Police or the ACC, as the case requires—a
- 31 copy of the variation;
- 32 (j) if an account takeover warrant issued in response to an
- 33 application made by a law enforcement officer of the
- 34 Australian Federal Police or the ACC, as the case requires,
- 35 was revoked—a copy of the revocation;
- 36 (k) each written record made under subsection 3ZZUN(5);
- 37 (l) a copy of each report given to the Minister and the
- 38 Ombudsman under section 3ZZVL.

3ZZVP Register of applications for account takeover warrants and emergency authorisations

- (1) The chief officer of the Australian Federal Police or the ACC must cause to be kept a register of:
 - (a) applications for account takeover warrants made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires; and
 - (b) applications for emergency authorisations made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires.
- (2) The register is to specify, for each account takeover warrant sought by a law enforcement officer of the Australian Federal Police or the ACC, as the case requires:
 - (a) the date the warrant was issued or refused; and
 - (b) the date of the application for the warrant; and
 - (c) whether the application for the warrant was a formal application or an urgent application; and
 - (d) the name of the magistrate who issued or refused to issue the warrant; and
 - (e) the name of the applicant for the warrant; and
 - (f) if the warrant was issued:
 - (i) the name of the executing officer; and
 - (ii) the alleged relevant offence, or alleged relevant offences, in respect of which the warrant was issued; and
 - (iii) the period during which the warrant is in force; and
 - (iv) details of any variations or extensions of the warrant; and
 - (v) whether the warrant has expired or been revoked.
- (3) The register is to specify, for each emergency authorisation sought by a law enforcement officer of the Australian Federal Police or the ACC, as the case requires:
 - (a) the date the authorisation was given or refused; and
 - (b) the name of the appropriate authorising officer who gave or refused to give the authorisation; and
 - (c) if the authorisation was given:

- 1 (i) the name of the law enforcement officer to whom the
- 2 authorisation was given; and
- 3 (ii) the alleged relevant offence, or alleged relevant
- 4 offences, in respect of which the authorisation was
- 5 given; and
- 6 (iii) the date on which the application for approval of the
- 7 giving of the authorisation was made; and
- 8 (iv) whether that application for approval of the giving of
- 9 the authorisation was successful or not.

10 (4) A register kept under this section is not a legislative instrument.

11 **Division 7—Inspections**

12 **3ZZVQ Appointment of inspecting officers**

13 The Ombudsman may, by writing, appoint members of the
14 Ombudsman's staff to be inspecting officers for the purposes of
15 this Part.

16 **3ZZVR Inspection of records by the Ombudsman**

- 17 (1) The Ombudsman must, from time to time and at least once every
- 18 12 months, inspect the records of the Australian Federal Police and
- 19 the ACC to determine the extent of compliance with this Part by:
 - 20 (a) the Australian Federal Police or the ACC, as the case
 - 21 requires; and
 - 22 (b) law enforcement officers of the Australian Federal Police or
 - 23 the ACC, as the case requires.
- 24 (2) For the purpose of an inspection under this section, the
- 25 Ombudsman:
 - 26 (a) may, after notifying the chief officer of the Australian
 - 27 Federal Police or the ACC, enter at any reasonable time
 - 28 premises occupied by the Australian Federal Police or the
 - 29 ACC, as the case requires; and
 - 30 (b) is entitled to have full and free access at all reasonable times
 - 31 to all records of the Australian Federal Police or the ACC
 - 32 that are relevant to the inspection; and

-
- 1 (c) may require a member of staff of the Australian Federal
2 Police or the ACC to give the Ombudsman any information
3 that the Ombudsman considers necessary, so long as:
4 (i) the information is in the member's possession, or the
5 member has access to the information; and
6 (ii) the information is relevant to the inspection; and
7 (d) may, despite any other law, make copies of, and take extracts
8 from, records of the Australian Federal Police or the ACC.
- 9 (3) The chief officer of the Australian Federal Police or the ACC must
10 ensure that members of staff of the Australian Federal Police or the
11 ACC, as the case requires, give the Ombudsman any assistance the
12 Ombudsman reasonably requires to enable the Ombudsman to
13 perform functions under this section.

14 **3ZZVS Power to obtain relevant information**

- 15 (1) If the Ombudsman has reasonable grounds to believe that a law
16 enforcement officer of the Australian Federal Police or the ACC is
17 able to give information relevant to an inspection under this
18 Division of the records of the Australian Federal Police or the
19 ACC, subsections (2) and (3) have effect.
- 20 (2) The Ombudsman may, by writing given to the law enforcement
21 officer, require the officer to give the information to the
22 Ombudsman:
23 (a) by writing signed by the officer; and
24 (b) at a specified place and within a specified period.
- 25 (3) The Ombudsman may, by writing given to the law enforcement
26 officer, require the officer to attend:
27 (a) before a specified inspecting officer; and
28 (b) at a specified place; and
29 (c) within a specified period or at a specified time on a specified
30 day;
31 to answer questions relevant to the inspection.
- 32 (4) If the Ombudsman:
33 (a) has reasonable grounds to believe that a law enforcement
34 officer of the Australian Federal Police or the ACC is able to

- 1 give information relevant to an inspection under this Division
2 of the records of the Australian Federal Police or the ACC;
3 and
4 (b) does not know the officer's identity;
5 the Ombudsman may, by writing given to the chief officer of the
6 Australian Federal Police or the ACC, as the case requires, require
7 the chief officer, or a person nominated by the chief officer, to
8 attend:
9 (c) before a specified inspecting officer; and
10 (d) at a specified place; and
11 (e) within a specified period or at a specified time on a specified
12 day;
13 to answer questions relevant to the inspection.
- 14 (5) The place, and the period or the time and day, specified in a
15 requirement under this section, must be reasonable having regard
16 to the circumstances in which the requirement is made.

17 **3ZZVT Offence**

- 18 A person commits an offence if:
19 (a) the person is required under section 3ZZVS to attend before
20 an inspecting officer, to give information or to answer
21 questions; and
22 (b) the person refuses or fails to do so.
- 23 Penalty: Imprisonment for 6 months.

24 **3ZZVU Ombudsman to be given information and access despite**
25 **other laws**

- 26 (1) Despite any other law, a person is not excused from giving
27 information, answering a question, or giving access to a document,
28 as and when required under this Division, on the ground that giving
29 the information, answering the question, or giving access to the
30 document, as the case may be:
31 (a) would contravene a law; or
32 (b) would be contrary to the public interest; or
33 (c) might tend to incriminate the person; or
34 (d) would disclose one of the following:
-

-
- 1 (i) a legal advice given to a Minister, a Department or a
2 prescribed authority;
- 3 (ii) a communication between an officer of a Department or
4 of a prescribed authority and another person or body,
5 being a communication protected against disclosure by
6 legal professional privilege.
- 7 (2) However, if the person is an individual:
- 8 (a) the information, the answer, or the fact that the person has
9 given access to the document, as the case may be; and
- 10 (b) any information or thing (including a document) obtained as
11 a direct or indirect consequence of giving the information,
12 answering the question or giving access to the document;
- 13 is not admissible in evidence against the person except in a
14 proceeding by way of a prosecution for an offence against
15 section 3ZZVH of this Act or Part 7.4 or 7.7 of the *Criminal Code*.
- 16 (3) If, at general law, an individual would otherwise be able to claim
17 the privilege against self-exposure to a penalty (other than a
18 penalty for an offence) in relation to giving information, answering
19 a question, or giving access to a document, as and when required
20 under this Division, the individual is not excused from giving the
21 information, answering the question, or giving access to the
22 document, as the case may be, on that ground.
- 23 Note: A body corporate is not entitled to claim the privilege against
24 self-exposure to a penalty.
- 25 (4) Nothing in section 3ZZVH or in any other law prevents a law
26 enforcement officer of the Australian Federal Police or the ACC
27 from:
- 28 (a) giving information to an inspecting officer (whether orally or
29 in writing and whether or not in answer to a question); or
- 30 (b) giving access to a record of the Australian Federal Police or
31 the ACC, as the case requires, to an inspecting officer;
- 32 for the purposes of an inspection under this Division of the records
33 of the Australian Federal Police or the ACC, as the case requires.
- 34 (5) Nothing in section 3ZZVH or in any other law prevents a law
35 enforcement officer from making a record of information, or
36 causing a record of information to be made, for the purposes of
37 giving the information to a person as permitted by subsection (4).
-

1 (6) The fact that a person is not excused under subsection (1) or (3)
2 from giving information, answering a question or giving access to
3 a document does not otherwise affect a claim of legal professional
4 privilege that anyone may make in relation to that information,
5 answer or document.

6 (7) In this section:

7 *prescribed authority* has the same meaning as in the *Ombudsman*
8 *Act 1976*.

9 **3ZZVV Delegation by Ombudsman**

10 (1) The Ombudsman may, by writing, delegate to an APS employee
11 responsible to the Ombudsman all or any of the Ombudsman's
12 functions or powers under this Division, other than
13 section 3ZZVX.

14 (2) A delegate must, on request by a person affected by the exercise of
15 any power delegated to the delegate, produce the instrument of
16 delegation, or a copy of the instrument, for inspection by the
17 person.

18 **3ZZVW Ombudsman not to be sued**

19 The Ombudsman, an inspecting officer, or a person acting under an
20 inspecting officer's direction or authority, is not liable to an action,
21 suit or proceeding for or in relation to an act done, or omitted to be
22 done, in good faith in the performance or exercise, or the purported
23 performance or exercise, of a function or power conferred by this
24 Division.

25 **3ZZVX Report on inspection**

26 (1) The Ombudsman must make a written report to the Minister at 12
27 monthly intervals on the results of each inspection under
28 section 3ZZVR.

29 (2) The report must not include information which, if made public,
30 could reasonably be expected to:

31 (a) prejudice an investigation or prosecution; or

- 1 (b) compromise any law enforcement agency's operational
- 2 activities or methodologies.
- 3 (3) The Minister must cause a copy of the report to be tabled in each
- 4 House of the Parliament within 15 sitting days of that House after
- 5 the Minister receives the report.

6 **Division 8—Miscellaneous**

7 **3ZZVY Minor defects in connection with account takeover warrant**

- 8 (1) If:
- 9 (a) information is purportedly obtained under an account
- 10 takeover warrant; and
- 11 (b) there is a defect or irregularity in relation to the warrant; and
- 12 (c) but for that defect or irregularity, the warrant would be a
- 13 sufficient authority for obtaining the information;
- 14 then:
- 15 (d) obtaining the information is taken to be as valid; and
- 16 (e) the information obtained may be dealt with, or given in
- 17 evidence in any proceeding;
- 18 as if the warrant did not have that defect or irregularity.
- 19 (2) A reference in subsection (1) to a defect or irregularity in relation
- 20 to the warrant is a reference to a defect or irregularity (other than a
- 21 substantial defect or irregularity):
- 22 (a) in, or in connection with the issue of, a document purporting
- 23 to be that warrant; or
- 24 (b) in connection with the execution of that warrant or the
- 25 purported execution of a document purporting to be that
- 26 warrant.

27 **3ZZVZ Evidentiary certificates**

- 28 (1) A law enforcement officer may issue a written certificate signed by
- 29 the officer setting out any facts the officer considers relevant with
- 30 respect to:
- 31 (a) anything done by the law enforcement officer, or by a person
- 32 assisting or providing technical expertise to the law

1 enforcement officer, in connection with the execution of an
2 account takeover warrant; or

3 (b) anything done by the law enforcement officer in connection
4 with:

5 (i) the communication by a person to another person; or

6 (ii) the making use of; or

7 (iii) the making of a record of; or

8 (iv) the custody of a record of;

9 information obtained under an account takeover warrant.

10 (2) A certificate issued under subsection (1) is admissible in evidence
11 in any proceedings as prima facie evidence of the matters stated in
12 the certificate.

13 **3ZZWA Compensation for property loss or serious damage**

14 (1) If a person suffers:

15 (a) loss of or serious damage to property; or

16 (b) personal injury;

17 in the course of, or as a direct result of, the execution of an account
18 takeover warrant, the Commonwealth is liable to pay to the person
19 compensation as agreed between the Commonwealth and the
20 person or, in default of agreement, as determined by action against
21 the Commonwealth in:

22 (c) the Federal Court of Australia; or

23 (d) the Supreme Court of a State or Territory.

24 (2) Subsection (1) does not apply if the person suffered the loss,
25 damage or injury in the course of, or as a direct result of, engaging
26 in any criminal activity.

27 ***National Emergency Declaration Act 2020***

28 **5 Paragraph 15(8)(a)**

29 After “IAAA,” insert “IAAC,”.

Schedule 3A—Reviews

Independent National Security Legislation Monitor Act 2010

1 At the end of subsection 6(1)

Add:

; (e) the function conferred by subsection (1E).

2 Before subsection 6(2)

Insert:

(1E) The Independent National Security Legislation Monitor must:

- (a) review the operation, effectiveness and implications of the amendments made by Schedules 1, 2 and 3 to the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*; and
- (b) commence to do so before the end of the 3-year period beginning on the day that Act receives the Royal Assent.

Intelligence Services Act 2001

3 After paragraph 29(1)(bc)

Insert:

- (bcaa) if the Committee resolves to do so—to commence, as soon as practicable after the fourth anniversary of the day the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* receives the Royal Assent, a review of the operation, effectiveness and implications of the amendments made by Schedules 1, 2 and 3 to that Act; and

Schedule 4—Controlled operations

Crimes Act 1914

1 Paragraph 15GI(2)(d)

Before “that the operation”, insert “so far as the conduct involved in the controlled operation is not conducted online—”.

2 Paragraph 15GQ(2)(d)

Before “that the operation”, insert “so far as the conduct involved in the controlled operation is not conducted online—”.

3 Paragraph 15GV(2)(d)

Before “that the operation”, insert “so far as the conduct involved in the controlled operation is not conducted online—”.

Schedule 5—Minor amendments

Surveillance Devices Act 2004

1 Subsection 43A(10)

Omit “of a vessel”, substitute “on a vessel”.

2 Before paragraph 45(4)(a)

Insert:

(aa) the use, recording, communication or publication of protected information in connection with the administration or execution of this Act; or

3 Subparagraph 45(4)(e)(i)

After “by”, insert “the Director-General (within the meaning of the *Australian Security Intelligence Organisation Act 1979*)”.

4 Subparagraph 45(4)(e)(i)

Omit “(within the meaning of the *Australian Security Intelligence Organisation Act 1979*)”, substitute “(within the meaning of that Act)”.

5 Subparagraph 45(4)(e)(ii)

After “by”, insert “the agency head (within the meaning of the *Intelligence Services Act 2001*), or”.

6 Subparagraph 45(4)(e)(ii)

Omit “(within the meaning of the *Intelligence Services Act 2001*)”, substitute “(within the meaning of that Act)”.

Telecommunications (Interception and Access) Act 1979

7 Paragraph 63AB(2)(g)

Repeal the paragraph, substitute:

(g) activities that pose a risk, or are likely to pose a risk, to the operational security (within the meaning of the *Intelligence Services Act 2001*) of ASIS (within the meaning of that Act);

- 1 (ga) activities that pose a risk, or are likely to pose a risk, to the
2 operational security (within the ordinary meaning of that
3 expression) of the Organisation or of AGO or ASD (within
4 the meanings of the *Intelligence Services Act 2001*);

5 **8 Paragraph 63AC(2)(g)**

6 Repeal the paragraph, substitute:

- 7 (g) activities that pose a risk, or are likely to pose a risk, to the
8 operational security (within the meaning of the *Intelligence*
9 *Services Act 2001*) of ASIS (within the meaning of that Act);
10 (ga) activities that pose a risk, or are likely to pose a risk, to the
11 operational security (within the ordinary meaning of that
12 expression) of the Organisation or of AGO or ASD (within
13 the meanings of the *Intelligence Services Act 2001*);
14