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

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

The Parliament of Australia enacts:

1 Short title

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

2 Commencement

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

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	
2. Schedule 1	The day after this Act receives the Royal Assent.	
3. Schedule 2	Immediately after the commencement of the provisions covered by table item 2.	
4. Schedules 3, 3A, 4 and 5	The day after this Act receives the Royal Assent.	

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

(2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

3 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

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

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

Procedure for making applications

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

(3) An application:

(a) must specify:

(i) the name of the applicant; and

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

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

(i) the grounds on which the warrant is sought; and

(ii) the things proposed to be authorised by the warrant in accordance with section 27KE; and

(iii) an assessment of how disruption of data held in the target computer is likely to substantially assist as described in paragraph (1)(c), to the extent that such an assessment is possible; and

(iv) an assessment of the likelihood that disruption of data held in the target computer will substantially assist as described in paragraph (1)(c), to the extent that such an assessment is possible.

Unsworn applications

(4) If a law enforcement officer believes that:

(a) immediate disruption of data held in the target computer referred to in subsection (1) is likely to substantially assist as described in paragraph (1)(c); and

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

an application for a warrant under subsection (1) may be made before an affidavit is prepared or sworn.

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

(a) provide as much information as the eligible Judge or nominated 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

disruption warrant unless the endorsing officer is satisfied that the making of the application is appropriate in all the circumstances.

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

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

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

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

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

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

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

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

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

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

(c) the chief officer is satisfied that each person in that class has completed all current internal training requirements relating

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

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

27KBB Endorsement of application—Australian Crime Commission

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

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

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

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

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

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

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

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

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

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

(a) each person in that class is an executive level member of the staff of the Australian Crime Commission; and

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

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

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

27KC Determining the application

(1) An eligible Judge or a nominated AAT member may issue a data disruption warrant if satisfied:

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

(b) the disruption of data authorised by the warrant is reasonably necessary and proportionate, having regard to the offences referred to in paragraph 27KA(1)(c); and

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

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

(2) In determining whether a data disruption warrant should be issued, the eligible Judge or nominated AAT member must have regard to:

(a) the nature and gravity of the conduct constituting the offences referred to in paragraph 27KA(1)(c); and

(b) the likelihood that the disruption of data authorised by the warrant will frustrate the commission of the offences referred to in paragraph 27KA(1)(c); and

(c) the existence of any alternative means of frustrating the commission of the offences referred to in paragraph 27KA(1)(c); and

(ca) the nature of the things proposed to be authorised by the warrant in accordance with section 27KE; and

(cb) the extent to which the execution of the warrant is likely to result in access to, or disruption of, data of persons lawfully using a computer, and any privacy implications (to the extent known) resulting from that access or disruption; and

(cc) any steps that are proposed to be taken to avoid or minimise the extent to which the execution of the warrant is likely to impact on persons lawfully using a computer; and

(cd) the extent to which the execution of the warrant is likely to cause a person to suffer a temporary loss of:

(i) money; or

(ii) digital currency; or

(iii) property (other than data);

so far as that matter is known to the eligible Judge or nominated AAT member; and

(ce) if:

(i) the eligible Judge or nominated AAT member believes on reasonable grounds that the data covered by the warrant (within the meaning of section 27KE) is data of a person who is working in a professional capacity as a journalist or of an employer of such a person; and

(ii) each of the offences referred to in paragraph 27KA(1)(c) is an offence against a secrecy provision;

whether the public interest in issuing the warrant outweighs:

(iii) the public interest in protecting the confidentiality of the identity of the journalist's source; and

(iv) the public interest in facilitating the exchange of information between journalists and members of the

public so as to facilitate reporting of matters in the public interest; and

(d) any previous warrant sought or issued under this Division in relation to the alleged relevant offences referred to in paragraph 27KA(1)(c).

(3) For the purposes of having regard to the nature and gravity of the conduct constituting the offences referred to in paragraph 27KA(1)(c), the eligible Judge or a nominated AAT member must give weight to the following matters:

(a) whether that conduct amounts to:

(i) an activity against the security of the Commonwealth; or

(ii) an offence against Chapter 5 of the *Criminal Code*;

(b) whether that conduct amounts to:

(i) an activity against the proper administration of Government; or

(ii) an offence against Chapter 7 of the *Criminal Code*;

(c) whether that conduct:

(i) causes, or has the potential to cause, serious violence, or serious harm, to a person; or

(ii) amounts to an offence against Chapter 8 of the *Criminal Code*;

(d) whether that conduct:

(i) causes, or has the potential to cause, a danger to the community; or

(ii) amounts to an offence against Chapter 9 of the *Criminal Code*;

(e) whether that conduct:

(i) causes, or has the potential to cause, substantial damage to, or loss of, data, property or critical infrastructure; or

(ii) amounts to an offence against Chapter 10 of the *Criminal Code*;

(f) whether that conduct involves, or is related to, the commission of:

(i) transnational crime; or

(ii) serious crime; or

(iii) organised crime;

that is not covered by any of the preceding paragraphs.

(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

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

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

(2) A warrant may only be issued for a period of no more than 90 days.

Note: The access to, or disruption of, data held in the target computer pursuant to a warrant may be discontinued earlier—see section 27KH.

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

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

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

(a) inform the applicant of:

(i) the terms of the warrant; and

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

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

27KE What a data disruption warrant authorises

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

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

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

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

(c) using:

(i) the target computer; or

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

(iii) any other electronic equipment; or

(iv) a data storage device;

for the following purposes:

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

(vi) disrupting the relevant data at any time while the warrant is in force, if doing so is likely to assist in frustrating the commission of one or more relevant offences covered by the warrant;

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

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

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

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

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

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

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

(ii) is covered by the warrant;

(h) intercepting a communication passing over a telecommunications system, if the interception is for the

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

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

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

(3) If:

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

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

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

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

(a) access has been obtained to data; and

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

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

When data is covered by a warrant

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

When a relevant offence is covered by a warrant

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

Certain acts not authorised

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

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

Warrant must provide for certain matters

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

Concealment of access etc.

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

mentioned in paragraph (c), and returning the computer or other thing to that place;

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

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

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

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

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

at the following time:

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

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

(10) Subsection (9) does not authorise the doing of a thing that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

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

unless the doing of the thing is necessary to do one or more of the things specified in subsection (9); or

(b) cause any other material loss or damage to other persons lawfully using a computer, unless the loss or damage is reasonably necessary, and proportionate, to do one or more of the things specified in the warrant or authorised by subsection (9).

(11) If a computer or another thing is removed from a place in accordance with paragraph (9)(f), the computer or thing must be returned to the place as soon as is reasonably practicable to do so

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

Statutory conditions

(12) A data disruption warrant is subject to the following conditions:

(a) the warrant must not be executed in a manner that results in loss or damage to data unless the damage is reasonably necessary, and proportionate, to do one or more of the things specified in the warrant or authorised by subsection (9);

(b) the warrant must not be executed in a manner that causes a person to suffer a permanent loss of:

(i) money; or

(ii) digital currency; or

(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

subsection 27KC(1) still exist, having regard to the matters in subsection 27KC(2).

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

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

27KG Revocation of data disruption warrant

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

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

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

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

(5) If:

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

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

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

27KH Discontinuance of access and disruption under warrant

Scope

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

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

(c) the circumstances are so serious and the matter is of such urgency that disruption of data held in the target computer is warranted; and

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

(1D) The target computer mentioned in subsection (1C) may be any one or more of the following:

(a) a particular computer;

(b) a computer on particular premises;

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

16 Subsections 28(3) and (4)

Omit "or (1A)", substitute ", (1A) or (1C)".

17 At the end of section 28

Add:

(4A) In deciding whether to give an emergency authorisation for disruption of data held in a computer, the appropriate authorising officer must have regard to:

(a) the extent to which the execution of the emergency authorisation is likely to result in access to, or disruption of, data of persons lawfully using a computer; and

(b) whether the likely impact of the execution of the emergency authorisation on persons lawfully using a computer is proportionate, having regard to the risk of serious violence or substantial damage referred to in paragraph (1C)(a).

(4B) Subsection (4A) does not limit the matters to which the appropriate authorising officer may have regard.

Statutory conditions—disruption of data held in a computer

(5) An emergency authorisation for disruption of data held in a computer is subject to the following conditions:

(a) the authorisation must not be executed in a manner that results in damage to data unless the damage is reasonably necessary and proportionate, having regard to the risk of

serious violence or substantial damage referred to in paragraph (1C)(a);

(b) the authorisation must not be executed in a manner that causes a person to suffer a permanent loss of:

(i) money; or

(ii) digital currency; or

(iii) property (other than data).

18 After subsection 32(2A)

Insert:

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

19 After subsection 32(3A)

Insert:

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

20 Subsection 32(4)

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

21 After subsection 33(2A)

Insert:

(2B) In the case of an application for an emergency authorisation for disruption of data held in a computer, the application:

(a) must specify:

(i) the name of the applicant for the approval; and

(ii) if a warrant is sought—the nature and duration of the warrant; and

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

(c) must be accompanied by a copy of the written record made under section 31 in relation to the emergency authorisation.

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

(b) disruption of data held in the target computer mentioned in that subsection may have helped reduce the risk; and

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

(2) If, under subsection (1), the eligible Judge or nominated AAT member approves the giving of an emergency authorisation, the eligible Judge or nominated AAT member may:

(a) unless paragraph (b) applies—issue a data disruption warrant relating to the continued access to, and disruption of, data held in the relevant target computer as if the application for the approval were an application for a data disruption warrant under Division 5 of Part 2; or

(b) if the eligible Judge or nominated AAT member is satisfied that, since the application for the emergency authorisation, the activity that required access to, and disruption of, data held in the relevant target computer has ceased—order that access to, and disruption of, data held in that computer cease.

(3) If, under subsection (1), the eligible Judge or nominated AAT member does not approve the giving of an emergency authorisation, the eligible Judge or nominated AAT member may:

(a) order that access to, and disruption of, data held in the relevant target computer cease; or

(b) if the eligible Judge or nominated AAT member is of the view that, although the situation did not warrant the emergency authorisation at the time that authorisation was given, the use of a data disruption warrant under Division 5 of Part 2 is currently justified—issue a data disruption warrant relating to the subsequent access to, and disruption of, such data as if the application for the approval were an application for a data disruption warrant under Division 5 of Part 2.

(4) In any case, the eligible Judge or nominated AAT member may order that any information obtained from or relating to the exercise of powers under the emergency authorisation, or any record of that information, be dealt with in a manner specified in the order, so long as the manner does not involve the destruction of that information.

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.

(2) If:

(a) an application is made under section 33 by an appropriate authorising officer for approval of the giving of an emergency authorisation; and

(b) the emergency authorisation was given in response to an application under subsection 28(1C); and

(c) before the completion of consideration of that section 33 application, it becomes apparent to the applicant that there will be a need for access to, and disruption of, data held in a computer:

(i) in a foreign country; or

(ii) on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limits of the territorial sea of Australia;

the eligible Judge or nominated AAT member to whom the section 33 application was made must not permit any data disruption warrant issued on consideration of that section 33 application to authorise that access and disruption unless the eligible Judge or nominated AAT member is satisfied that the access and disruption has been agreed to by an appropriate consenting official of the foreign country.

(3) If:

(a) a data disruption warrant has been issued; and

(b) after the issue of the warrant, it becomes apparent to the law enforcement officer primarily responsible for executing the warrant that there will be a need for access to, and disruption of, data held in a computer that is:

(i) in a foreign country; or

(ii) on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limits of the territorial sea of Australia;

the warrant is taken to permit that access and disruption if, and only if, the access and or disruption has been agreed to by an appropriate consenting official of the foreign country.

(4) Subsections (1), (2) and (3) do not apply to a data disruption warrant authorising access to, and disruption of, data if:

(a) the person, or each of the persons, responsible for executing the warrant will be physically present in Australia; and

(b) the location where the data is held is unknown or cannot reasonably be determined.

(5) Despite subsections (1), (2) and (3), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the contiguous zone of Australia; and

(b) the relevant offences in respect of which it becomes apparent that access to, and disruption of, data held in a computer on the vessel will be required are offences relating to the customs, fiscal, immigration or sanitary laws of Australia;

there is no requirement for the agreement of an appropriate consenting official of the foreign country concerned in relation to that access or disruption while the vessel is in such waters.

(6) Despite subsections (1), (2) and (3), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the Australian fishing zone; and

(b) the relevant offences in respect of which it becomes apparent that access to, and disruption of, data held in a computer on the vessel will be required are offences against section 100, 100A, 100B, 101, 101A or 101AA of the *Fisheries Management Act 1991* or section 46A, 46B, 46C, 46D, 49A or 51A of the *Torres Strait Fisheries Act 1984*;

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

(7) As soon as practicable after the commencement of access to, and disruption of, data held in a computer under the authority of a data disruption warrant in circumstances where consent to that access or disruption is required:

(a) in a foreign country; or

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

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

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

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

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

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

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

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

Insert:

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

(i) a data disruption warrant; or

(ii) an emergency authorisation for disruption of data held in a computer; or

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

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

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

Add "or".

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

Insert:

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

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

Omit "such".

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

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

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

proceeding includes a proceeding before a court, tribunal or Royal Commission.

40 After subsection 49(2C)

Insert:

(2D) In the case of:

(a) a data disruption warrant for disruption of data held in a computer; or

(b) an emergency authorisation for disruption of data held in a computer;

the report must:

(c) state whether the warrant or authorisation was executed; and

(d) if so:

(i) state the name of the person primarily responsible for the execution of the warrant or authorisation; and

(ii) state the name of each person involved in accessing or disrupting data under the warrant or authorisation; and

(iii) state the period during which the data was accessed or disrupted; and

(iv) state the name, if known, of any person whose data was accessed or disrupted; and

(v) give details of any premises at which the computer was located; and

(vi) give details of the benefit of the use of the warrant or authorisation in frustrating criminal activity; and

(vii) give details of the access to, and disruption of, data under the warrant or authorisation; and

(viii) give details of the compliance with the conditions (if any) to which the warrant or authorisation was subject; and

(e) if the warrant or authorisation was extended or varied, state:

(i) the number of extensions or variations; and

(ii) the reasons for them.

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

(iv) a data storage device;

for the purpose of obtaining access to, or disrupting, data that is held in the computer; and

(b) the use of the computer, facility, equipment or device, as the case may be, was authorised by an emergency authorisation for disruption of data held in a computer; and

(c) the giving of the emergency authorisation was not approved under section 35B;

the Commonwealth is liable to pay to the person who has suffered the loss or injury:

(d) such compensation as is agreed on between the Commonwealth and that person; or

(e) in default of such an agreement—such compensation as is determined by action against the Commonwealth in a court of a State or Territory that has jurisdiction in relation to the matter.

47 After section 64A

Insert:

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

(1) A law enforcement officer of the Australian Federal Police or the Australian Crime Commission (or another person on the officer's behalf) may apply to an eligible Judge or to a nominated AAT member for an order (the ***assistance order***) requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the law enforcement officer to do one or more of the following:

(a) disrupt data held in a computer that is the subject of:

(i) a data disruption warrant; or

(ii) an emergency authorisation given in response to an application under subsection 28(1C);

(b) access data that is held in the computer described in paragraph (a);

(c) copy data held in the computer described in paragraph (a) to a data storage device;

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

(i) data held in the computer described in paragraph (a); or

(ii) data held in a data storage device to which the data was copied as described in paragraph (c).

Grant of assistance order

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

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

(i) likely to substantially assist in frustrating the commission of the offences that are covered by the warrant (within the meaning of section 27KE); and

(ii) justifiable and proportionate, having regard to those offences; and

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

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

(i) the nature and gravity of the conduct constituting the offences referred to in paragraph 27KA(1)(c); and

(ii) the likely impact of compliance with the assistance order on the specified person, so far as that matter is known to the eligible Judge or nominated AAT member; and

(iii) the likely impact of compliance with the assistance order on other persons (including persons who may lawfully be using the computer), so far as that matter is known to the eligible Judge or nominated AAT member; and

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

(i) there is an imminent risk of serious violence to a person or substantial damage to property; and

(ii) disruption of data held in the computer is immediately necessary for the purpose of dealing with the risk; and

(ba) in a case where the computer is the subject of an emergency authorisation given in response to an application under subsection 28(1C)—the assistance order is reasonable and necessary to enable the emergency authorisation to be executed; and

(bb) in a case where the computer is the subject of an emergency authorisation given in response to an application under subsection 28(1C)—the assistance order is justifiable and proportionate, having regard to:

(i) the risk of serious violence or substantial damage referred to in paragraph 28(1C)(a); and

(ii) the likely impact of compliance with the assistance order on the specified person, so far as that matter is known to the eligible Judge or nominated AAT member; and

(iii) the likely impact of compliance with the assistance order on other persons (including persons who may lawfully be using the computer), so far as that matter is known to the eligible Judge or nominated AAT member; and

(c) in a case where:

(i) the computer is the subject of a data disruption warrant; and

(ii) the assistance order requires the specified person to provide information or assistance to allow the law enforcement officer to do a thing referred to in paragraph (1)(b), (c) or (d) in relation to data;

doing the thing is for the purpose of determining whether the data is covered by the warrant (within the meaning of section 27KE); and

(d) in a case where:

(i) the computer is the subject of an emergency authorisation given in response to an application under subsection 28(1C); and

(ii) the assistance order requires the specified person to provide information or assistance to allow the law enforcement officer to do a thing referred to in paragraph (1)(b), (c) or (d) in relation to data;

doing the thing is for the purpose of determining whether disruption of the data is immediately necessary for the purpose of dealing with an imminent risk of serious violence to a person or substantial damage to property; and

(e) the specified person is:

(i) in a case where the computer is the subject of a data disruption warrant—reasonably suspected of having committed any of the relevant offences referred to in paragraph 27KA(1)(c); or

(ii) in a case where the computer is the subject of emergency authorisation—reasonably suspected of having committed the relevant offence referred to in subsection 28(1C); or

(iii) the owner or lessee of the computer; or

(iv) an employee of the owner or lessee of the computer; or

(v) a person engaged under a contract for services by the owner or lessee of the computer; or

(vi) a person who uses or has used the computer; or

(vii) a person who is or was a system administrator for the system including the computer; and

(f) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms or formed a part; or

(ii) measures applied to protect data held in the computer.

(2A) In determining whether the assistance order should be granted, the eligible Judge or nominated 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 64A of this Act; or

(c) an order under section 3LA or 3ZZVG of the *Crimes Act 1914*;

so far as that matter is known to the eligible Judge or nominated AAT member.

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

Duration of assistance order

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

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

Protection from civil liability

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

(a) in compliance with an assistance order; or

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

Offence

(3) A person commits an offence if:

(a) the person is subject to an order under this section; and

(b) the person is capable of complying with a requirement in the order; and

(c) the person omits to do an act; and

(d) the omission contravenes the requirement.

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

48 Paragraph 65(1A)(a)

After "computer access warrant", insert ", data disruption warrant".

49 After subsection 65(1A)

Insert:

(1B) If:

(a) data is disrupted purportedly under:
(i) a data disruption warrant; or
(ii) an emergency authorisation for disruption of data held in a computer; and
(b) there is a defect or irregularity in relation to the warrant or emergency authorisation; and
(c) but for that defect or irregularity, the warrant or emergency authorisation would be a sufficient authority for disrupting the data;

disruption of the data is taken to be as valid as if the warrant or emergency authorisation did not have that defect or irregularity.

50 Subsection 65(2)

Omit "or (1A)", substitute ", (1A) or (1B)".

51 After section 65B

Insert:

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

This Act does not prevent evidence obtained from access to, or disruption of, data under:

(a) a data disruption warrant; or
(b) an emergency authorisation for disruption of data held in a computer;

from being admissible as evidence in a proceeding relating to a relevant offence.

Telecommunications (Interception and Access) Act 1979

52 Subsection 5(1)

Insert:

data disruption intercept information means information obtained under a data disruption warrant by intercepting a communication 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;

(e) acting for, or on behalf of, a foreign power (within the meaning of the *Australian Security Intelligence Organisation Act 1979*);

(f) activities that are, or are likely to be, a threat to security;

(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);

(h) activities that pose a risk, or are likely to pose a risk, to the operational security (within the ordinary meaning of that expression) of the Organisation or of AGO or ASD (within the meanings of the *Intelligence Services Act 2001*);

(i) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);

(j) activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law (within the meaning of the *Charter of the United Nations Act 1945*).

(3) A person may, in connection with:

(a) the performance by an Ombudsman official of the Ombudsman official's functions or duties; or

(b) the exercise by an Ombudsman official of the Ombudsman official's powers;

communicate to the Ombudsman official, or make use of, or make a record of, data disruption intercept information.

(4) An Ombudsman official may, in connection with:

(a) the performance by the Ombudsman official of the Ombudsman official's functions or duties; or

(b) the exercise by the Ombudsman official of the Ombudsman official's powers;

communicate to another person, or make use of, or make a record of, data disruption intercept information.

(5) A person may, in connection with:

(a) the performance by an IGIS official of the IGIS official's functions or duties; or

(b) the exercise by an IGIS official of the IGIS official's powers;

communicate to the IGIS official, or make use of, or make a record of, data disruption intercept information.

(6) An IGIS official may, in connection with:

(a) the performance by the IGIS official of the IGIS official's functions or duties; or

(b) the exercise by the IGIS official of the IGIS official's powers;

communicate to another person, or make use of, or make a record of, data disruption intercept information.

(7) If:

(a) information was obtained by intercepting a communication passing over a telecommunications system; and

(b) the interception was purportedly for the purposes of doing a thing specified in a data disruption warrant; and

(c) the interception was not authorised by the data disruption warrant;

then:

(d) a person may, in connection with:

(i) the performance by an Ombudsman official of the Ombudsman official's functions or duties; or

(ii) the exercise by an Ombudsman official of the Ombudsman official's powers;

communicate to the Ombudsman official, or make use of, or make a record of, that information; and

(e) an Ombudsman official may, in connection with:

(i) the performance by the Ombudsman official of the Ombudsman official's functions or duties; or

(ii) the exercise by the Ombudsman official of the Ombudsman official's powers;

communicate to another person, or make use of, or make a record of, that information; and

(f) a person may, in connection with:

(i) the performance by an IGIS official of the IGIS official's functions or duties; or

(ii) the exercise by an IGIS official of the IGIS official's powers;

communicate to the IGIS official, or make use of, or make a record of, that information; and

(g) an IGIS official may, in connection with:

(i) the performance by the IGIS official of the IGIS official's functions or duties; or

(ii) the exercise by the IGIS official of the IGIS official's powers;

communicate to another person, or make use of, or make a record of, that information.

(8) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution for an offence against section 63 of this Act, an Ombudsman official or an IGIS official does not bear an evidential burden in relation to the matters in subsection (4), (6) or (7) of this section.

57 Paragraph 67(1)(a)

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

58 Section 68

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

59 Subsection 74(1)

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

60 Subsection 75(1)

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

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

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

62 After paragraph 108(2)(cb)

Insert:

(cc) accessing a stored communication under a data disruption 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

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

9 At the end of Part 2

Add:

Division 6—Network activity warrants

27KKA Sunsetting

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

27KK Application for network activity warrant

(1) The chief officer of the Australian Federal Police or the Australian Crime Commission may apply for the issue of a network activity warrant if the chief officer suspects on reasonable grounds that:

(a) a group of individuals is a criminal network of individuals; and

(b) access to data held in a computer (the ***target computer***) that is, from time to time, used, or likely to be used, by any of the individuals in the group will substantially assist in the collection of intelligence that:

(i) relates to the group or to any of the individuals in the group; and

(ii) is relevant to the prevention, detection or frustration of one or more kinds of relevant offences.

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

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

(b) the target computer can be identified; or

(c) the location of the target computer can be identified; or

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

Procedure for making applications

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

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

Unsworn applications

(5) If the chief officer of the Australian Federal Police or the Australian Crime Commission believes that:
(a) immediate access to data held in the target computer referred to in subsection (1) will substantially assist as described in paragraph (1)(b); and
(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made by the chief officer;
an application by the chief officer for a warrant under subsection (1) may be made before an affidavit is prepared or sworn.

(6) If subsection (5) applies, the applicant must:
(a) provide as much information as the eligible Judge or nominated 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

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

27KL Remote application

(1) If the chief officer of the Australian Federal Police or the Australian Crime Commission believes that it is impracticable for an application for a network activity warrant to be made in person, the application may be made under section 27KK by telephone, fax, email or any other means of communication.

(2) If transmission by fax is available and an affidavit has been prepared, the person applying must transmit a copy of the affidavit, whether sworn or unsworn, to the eligible Judge or to the nominated 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

(ii) is relevant to the prevention, detection or frustration of one or more kinds of relevant offences; and

(c) the likely intelligence value of any information sought to be obtained; and

(d) whether the things authorised by the warrant are proportionate to the likely intelligence value of any information sought to be obtained; and

(e) the existence of any alternative, or less intrusive, means of obtaining the information sought to be obtained; and

(f) the extent to which the execution of the warrant is likely to result in access to data of persons who are lawfully using a computer, and any privacy implications (to the extent known to the eligible Judge or nominated AAT member) resulting from that access; and

(fa) if:

(i) the eligible Judge or nominated AAT member believes on reasonable grounds that the data covered by the warrant (within the meaning of section 27KP) is data of a person who is working in a professional capacity as a journalist or of an employer of such a person; and

(ii) each of the offences referred to in paragraph 27KK(1)(b) is an offence against a secrecy provision;

whether the public interest in issuing the warrant outweighs:

(iii) the public interest in protecting the confidentiality of the identity of the journalist's source; and

(iv) the public interest in facilitating the exchange of information between journalists and members of the public so as to facilitate reporting of matters in the public interest; and

(g) any previous warrant sought or issued under this Division in relation to the group referred to in paragraph 27KK(1)(a).

(2A) For the purposes of having regard to the nature and gravity of the conduct constituting the kinds of offences in relation to which information will be obtained under the warrant, the eligible Judge or nominated AAT member must give weight to the following matters:

(a) whether that conduct amounts to:

(i) an activity against the security of the Commonwealth; or

(ii) an offence against Chapter 5 of the *Criminal Code*;

(b) whether that conduct amounts to:

(i) an activity against the proper administration of Government; or

(ii) an offence against Chapter 7 of the *Criminal Code*;

(c) whether that conduct:

(i) causes, or has the potential to cause, serious violence, or serious harm, to a person; or

(ii) amounts to an offence against Chapter 8 of the *Criminal Code*;

(d) whether that conduct:

(i) causes, or has the potential to cause, a danger to the community; or

(ii) amounts to an offence against Chapter 9 of the *Criminal Code*;

(e) whether that conduct:

(i) causes, or has the potential to cause, substantial damage to, or loss of, data, property or critical infrastructure; or

(ii) amounts to an offence against Chapter 10 of the *Criminal Code*;

(f) whether that conduct involves, or is related to, the commission of:

(i) transnational crime; or

(ii) serious crime; or

(iii) organised crime;

that is not covered by any of the preceding paragraphs.

(2B) Subsection (2A) does not limit the matters that may be considered by the eligible Judge or nominated AAT member.

(2C) To avoid doubt, this Act does not prevent a network activity warrant from being issued in a case where the conduct constituting the kinds of offences in relation to which information will be obtained under the warrant is not covered by subsection (2A).

(3) If a network activity warrant is issued in response to an application made by the chief officer of the Australian Federal Police or the Australian Crime Commission, the chief officer must:
  (a) notify the issue of the warrant to the Inspector-General of Intelligence and Security; and
  (b) do so within 7 days after the issue of the warrant.

(4) For the purposes of this section, ***secrecy provision*** means a provision of a law of the Commonwealth or of a State that prohibits:
  (a) the communication, divulging or publication of information; or
  (b) the production of, or the publication of the contents of, a document.

27KN What must a network activity warrant contain?

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

(ii) the purpose or purposes for which the surveillance device may be used under the warrant.

(2) A warrant may only be issued for a period of no more than 90 days.

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

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

(4) For the purposes of subparagraph (1)(b)(iii), a criminal network of individuals may be specified by identifying one or more matters or things that are sufficient to identify the criminal network of individuals.

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

(a) inform the applicant of:

(i) the terms of the warrant; and

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

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

27KP What a network activity warrant authorises

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

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

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

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

(c) using:

(i) the target computer; or

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

(iii) any other electronic equipment; or

(iv) a data storage device;

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

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

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

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

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

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

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

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

(ii) is covered by the warrant;

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

(i) using a surveillance device for the purposes of doing any thing specified in the warrant in accordance with this subsection;

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

Note: As a result of the warrant, a person who, by means of a telecommunications facility, obtains access to data stored in a computer will not commit an offence under Part 10.7 of the *Criminal*

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

(3) If:

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

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

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

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

(a) access has been obtained to data; and

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

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

When data is covered by a warrant

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

Certain acts not authorised

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

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

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

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

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

Warrant must provide for certain matters

(7) A network activity warrant must:

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

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

Concealment of access etc.

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

(a) a network activity warrant; or

(b) this subsection;

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

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

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

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

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

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

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

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

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

(i) using a surveillance device, if the use is for the purposes of doing any thing mentioned in this subsection;

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

at the following time:

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

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

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

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

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

unless the doing of the thing is necessary to do one or more of the things specified in subsection (8); or

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

(10) If a computer or another thing is removed from a place in accordance with paragraph (8)(f), the computer or thing must be returned to the place as soon as is reasonably practicable to do so once the computer or thing is no longer required for the purposes of doing any thing mentioned in paragraph (8)(c).

27KQ Extension and variation of network activity warrant

(1) If a network activity warrant was issued in response to an application by the chief officer of the Australian Federal Police or the Australian Crime Commission, the chief officer may apply, at any time before the expiry of the warrant:

(a) for an extension of the warrant for a period of no more than 90 days after the day the warrant would otherwise expire; or

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

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

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

(4) The eligible Judge or nominated AAT member may grant an application if satisfied that the matters referred to in subsection 27KM(1) still exist, having regard to the matters in subsection 27KM(2).

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

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

(7) If a network activity warrant is extended or varied in response to an application made by the chief officer of the Australian Federal Police or the Australian Crime Commission, the chief officer must:

(a) notify the extension or variation to the Inspector-General of Intelligence and Security; and

(b) do so within 7 days after the extension or variation.

27KR Revocation of network activity warrant

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

(2) If the circumstances set out in subsection 27KS(2) apply in relation to a network activity warrant:

(a) if the warrant was issued in response to an application made by the chief officer of the Australian Federal Police—the chief officer of the Australian Federal Police must, by instrument in writing, revoke the warrant; or

(b) if the warrant was issued in response to an application made by the chief officer of the Australian Crime Commission—the chief officer of the Australian Crime Commission must, by instrument in writing, revoke the warrant.

(3) The instrument revoking a warrant must be signed by the eligible Judge, the nominated AAT member, the chief officer of the Australian Federal Police or the chief officer of the Australian Crime Commission, as the case requires.

(4) If an eligible Judge or nominated AAT member revokes a warrant, the eligible Judge or nominated AAT member must give a copy of the instrument of revocation to:

(a) if the warrant was issued in response to an application made by the chief officer of the Australian Federal Police—the chief officer of the Australian Federal Police; or

(b) if the warrant was issued in response to an application made by the chief officer of the Australian Crime Commission—the chief officer of the Australian Crime Commission.

(5) If:

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

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

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

(6) If:

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

(b) an eligible Judge or nominated AAT member revokes the warrant;

the chief officer must:

(c) notify the revocation to the Inspector-General of Intelligence and Security; and

(d) do so within 7 days after the revocation.

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

(a) notify the revocation to the Inspector-General of Intelligence and Security; and

(b) do so within 7 days after the revocation.

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

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

27KT Relationship of this Division to parliamentary privileges and immunities

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

(a) each House of the Parliament;

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

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

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

Omit "or 43D", substitute ", 43D or 43E".

11 At the end of Part 5

Add:

43E Extraterritorial operation of network activity warrants

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

(a) in a foreign country; or

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

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

(2) If:

(a) a network activity warrant has been issued; and

(b) after the issue of the warrant, it becomes apparent to the law enforcement officer primarily responsible for executing the

warrant that there will be a need for access to data held in a computer that is:

(i) in a foreign country; or

(ii) on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limits of the territorial sea of Australia;

the warrant is taken to permit that access if, and only if, the access has been agreed to by an appropriate consenting official of the foreign country.

(3) Subsections (1) and (2) do not apply to a network activity warrant authorising access to data if:

(a) the person, or each of the persons, responsible for executing the warrant will be physically present in Australia; and

(b) the location where the data is held is unknown or cannot reasonably be determined.

(4) Despite subsections (1) and (2), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the contiguous zone of Australia; and

(b) the relevant offence in respect of which it becomes apparent that access to data held in a computer on the vessel will be required is an offence relating to the customs, fiscal, immigration or sanitary laws of Australia;

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

(5) Despite subsections (1) and (2), if:

(a) a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the Australian fishing zone; and

(b) the relevant offence in respect of which it becomes apparent that access to data held in a computer on the vessel will be required is an offence against section 100, 100A, 100B, 101, 101A or 101AA of the *Fisheries Management Act 1991* or

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

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

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

(a) in a foreign country; or

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

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

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

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

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

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

After "warrant", insert "(other than a network activity warrant)".

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

After "warrant", insert "(other than a network activity warrant)".

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

After "warrant", insert "(other than a network activity warrant)".

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

After "warrant", insert "(other than a network activity warrant)".

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

After "obtained", insert "(otherwise than purportedly under a network activity warrant)".

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

After "warrant" (last occurring), insert "(other than a network activity warrant)".

18 After section 44

Insert:

44A What is protected network activity warrant information?

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

(a) any information (other than network activity warrant intercept information) obtained from access to data under a network activity warrant; or

(b) any information obtained from the use of a surveillance device under a network activity warrant; or

(c) information relating to an application for, the issue of, the existence of, or the expiration of, a network activity warrant; or

(d) any information that is likely to enable the identification of:

(i) a criminal network of individuals specified in a network activity warrant; or

(ii) an individual in a criminal network of individuals specified in a network activity warrant; or

(iii) a computer specified in a network activity warrant; or

(iv) premises specified in a network activity warrant; or

(e) any other information obtained by a law enforcement officer:

(i) without the authority of a network activity warrant; or

(ii) in a case where the information was obtained, purportedly under a network activity warrant, through access to data held in a computer in a foreign country, or on a vessel or aircraft that is registered under the law of a foreign country and that is in or above waters beyond the outer limit of Australia's territorial sea—without the agreement of the appropriate consenting official of that foreign country, and of any other foreign country, whose agreement is required under section 43E;

in contravention of the requirement for a network activity warrant.

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

19 After section 45A

Insert:

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

(1) A person commits an offence if:

(a) the person uses, records, communicates or publishes any information; and

(b) the information is protected network activity warrant information; and

(c) the use, recording, communication or publication of the information is not permitted by this section.

Penalty: Imprisonment for 2 years.

(2) A person commits an offence if:

(a) the person uses, records, communicates or publishes any information; and

(b) the information is protected network activity warrant information; and

(c) the use, recording, communication or publication of the information is not permitted by this section; and

(d) the use, recording, communication or publication of the information:

(i) endangers the health or safety of any person; or

(ii) prejudices the effective conduct of an investigation into a relevant offence.

Penalty: Imprisonment for 10 years.

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

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

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

(b) the use, recording, communication or publication of any information that has been disclosed in proceedings in open court lawfully; or

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

(d) the communication to the Director-General (within the meaning of the *Australian Security Intelligence Organisation Act 1979*) of protected network activity warrant information that relates or appears to relate to any matter within the functions of that organisation; or

(e) the communication to the agency head (within the meaning of the *Intelligence Services Act 2001*) of an agency (within

the meaning of that Act) of protected network activity warrant information that relates or appears to relate to any matter within the functions of that agency; or

(f) the use, recording or communication of:

(i) protected network activity warrant information referred to in paragraph (d)—by the Director-General (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), an ASIO employee (within the meaning of that Act) or an ASIO affiliate (within the meaning of that Act); or

(ii) protected network activity warrant information referred to in paragraph (e)—by the agency head (within the meaning of the *Intelligence Services Act 2001*), or a staff member (within the meaning of that Act), of an agency (within the meaning of that Act);

in the performance of the official functions of the Director-General, ASIO employee, ASIO affiliate, agency head or staff member, as the case may be.

(5) Protected network activity warrant information (other than information that was obtained from the use of a surveillance device under a network activity warrant) may be used, recorded, communicated or published, or may be admitted in evidence, if it is necessary to do so for any of the following purposes:

(a) the purposes of the Australian Federal Police collecting, correlating, analysing or disseminating criminal intelligence in the performance of the functions conferred by section 8 of the *Australian Federal Police Act 1979*;

(b) the purposes of the Australian Crime Commission collecting, correlating, analysing or disseminating criminal intelligence in the performance of the functions conferred by section 7A of the *Australian Crime Commission Act 2002*;

(c) the purposes of the Australian Federal Police or the Australian Crime Commission making reports in relation to criminal intelligence;

(d) the making of an application for a warrant;

(e) the making of an application for the variation of a warrant;

(f) the making of an application for the extension of a warrant;

(g) the keeping of records and the making of reports by the Australian Federal Police or the Australian Crime Commission under Division 2;

(h) the purposes of an IGIS official exercising powers, or performing functions or duties, as an IGIS official;

(i) the purposes of an investigation of an offence against subsection (1) or (2);

(j) a proceeding relating to an offence against subsection (1) or (2).

(6) The definition of ***warrant*** in subsection 6(1) does not apply to paragraphs (5)(d), (e) and (f) of this section.

Note: This means that warrant has its ordinary meaning.

(7) Protected network activity warrant information that was obtained from the use of a surveillance device under a network activity warrant may be used, recorded, communicated or published, or may be admitted in evidence, if it is necessary to do so for any of the following purposes:

(a) the purposes of doing a thing authorised by a network activity warrant;

(b) the purposes of an IGIS official exercising powers, or performing functions or duties, as an IGIS official;

(c) the purposes of an investigation of an offence against subsection (1) or (2);

(d) a proceeding relating to an offence against subsection (1) or (2).

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

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

(10) Protected network activity warrant information may be admitted in evidence in:

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

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

(11) If:

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

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

(c) the information:

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

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

the information that has been so communicated:

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

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

20 After section 46

Insert:

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

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

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

(i) protected network activity warrant information; or

(ii) network activity warrant intercept information;

is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report; and

(b) must cause to be destroyed any record or report referred to in paragraph (a):

(i) as soon as practicable after the making of the record or report if the chief officer is satisfied that no civil or criminal proceeding to which the material contained in the record or report relates has been, or is likely to be, commenced and that the material contained in the record or report is not likely to be required in connection with an activity referred to in subsection 45B(4) or a purpose referred to in subsection 45B(5) or (7); and

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

(2) If an agency is not a law enforcement agency but, as described in subsection 45B(5) or (7), receives records or reports obtained by accessing data, or using a surveillance device, under a network activity warrant, the officer in charge of the agency:

(a) must ensure that every record or report that is so received is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report; and

(b) must cause to be destroyed any record or report referred to in paragraph (a):

(i) as soon as practicable after the receipt of the record or report by the agency if the officer in charge is satisfied that no civil or criminal proceeding to which the material contained in the record or report relates has been, or is likely to be, commenced and that the material contained in the record or report is not likely to be required in connection with an activity referred to in subsection 45B(4) or a purpose referred to in subsection 45B(5) or (7); and

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

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

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

Insert:

(ca) a network activity warrant; or

22 After subsection 49(2D)

Insert:

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

(a) state whether the warrant was executed; and

(b) if so:

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

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

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

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

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

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

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

(viii) give details of the extent to which the execution of the warrant has assisted the agency in carrying out its functions; and

(ix) give details of the communication of information obtained by accessing data under the warrant to persons other than officers of the agency; and

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

(xi) give details of the information that was obtained from access to data under the warrant; and

(xii) give details of how the information that was obtained under the warrant was used; and

(xiii) give details of whether the information that was obtained under the warrant was destroyed or retained under section 46AA; and

(xiv) give details of any premises accessed, telecommunications intercepted or computers removed from premises under the warrant; and

(xv) give details of any activities undertaken under subsection 27KP(8) in relation to the warrant; and

(xvi) give details of any assistance orders made under subsection 64A(6A) in relation to the warrant; and

(c) if the warrant was extended or varied, state:

(i) the number of extensions or variations; and

(ii) the reasons for them.

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

(b) a thing mentioned in subsection 27KP(8) was done under the warrant after the 28-day period mentioned in paragraph 27KP(8)(k);

the chief officer must:

(c) notify the Inspector-General of Intelligence and Security of the fact that the thing was done under the warrant after the 28-day period mentioned in paragraph 27KP(8)(k); and

(d) do so within 7 days after the thing was done.

24 After paragraph 50(1)(eb)

Insert:

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

25 Paragraph 51(b)

Omit "or 27KG(4)", substitute ", 27KG(4) or 27KR(4)".

26 After paragraph 52(1)(h)

Insert:

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

27 Paragraph 52(1)(j)

After "46(1)(b)", insert "or 46AA(1)(b)".

28 After subsection 55(1)

Insert:

(1A) Subsection (1) does not apply to compliance with:

(a) Division 6 of Part 2 (network activity warrants); or

(b) the remaining provisions of this Act so far as they relate to network activity warrants.

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.

Protection from civil liability

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

(a) in compliance with an assistance order; or

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

32 Paragraph 65(1A)(a)

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.

38 After paragraph 60A(2)(f)

Insert:

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

Australian Human Rights Commission Act 1986

39 Subsection 3(1)

Insert:

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

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

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*.

40 At the end of subsection 11(3)

Add:

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

41 At the end of subsection 20(1)

Add:

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

42 After subsection 20(4B)

Insert:

(4C) If:

(a) a complaint has been made to the Commission in relation to:

(i) an act or practice of ACIC (except an act or practice of an examiner of ACIC performing functions and exercising powers as an examiner); or

(ii) an act or practice of the Australian Federal Police; and

(b) because the Commission is of the opinion that the subject matter of the complaint could be more effectively or conveniently dealt with by the Inspector-General of Intelligence and Security under the *Inspector-General of Intelligence and Security Act 1986*, the Commission decides not to inquire, or not to continue to inquire, into that act or practice;

the Commission must:

(c) consult the Inspector-General in relation to transferring the complaint or part of the complaint; and

(d) if the Inspector-General agrees to the transfer of the complaint or part of the complaint—transfer the complaint or part to the Inspector-General as soon as is reasonably practicable; and

(e) as soon as is reasonably practicable, take reasonable steps to give notice in writing to the complainant stating that the complaint or part has been so transferred; and

(f) give to the Inspector-General any information or documents that relate to the complaint or part and are in the possession, or under the control, of the Commission.

(4D) Without limiting subsection (4C), the Commission may consult with, and obtain an agreement from, the Inspector-General of Intelligence and Security by entering into an arrangement with the Inspector-General relating to the transfer of complaints (or parts) generally.

43 Subsection 46P(1) (note)

Omit "Note", substitute "Note 1".

44 At the end of subsection 46P(1)

Add:

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

45 Before section 47

Insert:

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

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

(a) made as referred to in paragraph 20(1)(b) of this Act; or

(b) lodged under section 46P of this Act.

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

(2) The determination has effect accordingly.

(3) The determination is not a legislative instrument.

46 Subsection 49(4A)

After "20(4A)(e)", insert "or (4C)(f)".

47 After subsection 49(4B)

Insert:

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

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

Insert:

(e) in relation to ACIC—the CEO of ACIC; or

(ea) in relation to the Australian Federal Police—the Commissioner of Police; or

53 Subsection 3(1)

Insert:

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

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

integrity body:

(a) means any of the following:

(i) the Ombudsman;

(ii) the Australian Human Rights Commission;

(iii) the Information Commissioner;

(iv) the Integrity Commissioner;

(v) the Inspector-General ADF; and

(b) for a complaint—has the meaning given by paragraph 11(4A)(a).

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

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

Repeal the definition, substitute:

intelligence agency means:

(a) ASIO, ASIS, AGO, DIO, ASD or ONI; or

(b) the following agencies that have an intelligence function:

(i) the Australian Federal Police;

(ii) ACIC.

55 Subsection 3(1)

Insert:

intelligence function:

(a) for ACIC—means:

(i) the collection, correlation, analysis, production and dissemination of intelligence obtained by ACIC from the execution of a network activity warrant; or

(ii) the performance of a function, or the exercise of a power, conferred on a law enforcement officer of ACIC by the network activity warrant provisions of the *Surveillance Devices Act 2004*; or

(b) for the Australian Federal Police—means:

(i) the collection, correlation, analysis, production and dissemination of intelligence obtained by the Australian Federal Police from the execution of a network activity warrant; or

(ii) the performance of a function, or the exercise of a power, conferred on a law enforcement officer of the Australian Federal Police by the network activity warrant provisions of the *Surveillance Devices Act 2004*.

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

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

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

(a) Division 6 of Part 2 of that Act; or

(b) the remaining provisions of that Act so far as they relate to network activity warrants.

56 After subsection 8(3)

Insert:

(3A) Subject to this section, the functions of the Inspector-General in relation to ACIC or the Australian Federal Police are:

(a) at the request of the Attorney-General or the responsible Minister; or

(b) of the Inspector-General's own motion; or

(c) in response to a complaint made to the Inspector-General;

to inquire into any of the following matters, to the extent that the matter relates to an intelligence function of that agency:

(d) the compliance by that agency with the laws of the Commonwealth and of the States and Territories;

(e) the compliance by that agency with directions or guidelines given to that agency by the responsible Minister;

(f) the propriety of particular activities of that agency;

(g) the effectiveness and appropriateness of the procedures of that agency relating to the legality or propriety of the activities of that agency;

(h) any matter that relates to an act or practice of that agency, referred to the Inspector-General by the Australian Human Rights Commission:

(i) that is or may be inconsistent with or contrary to any human right; or

(ii) that constitutes or may constitute discrimination; or

(iii) that is or may be unlawful under the *Age Discrimination Act 2004*, the *Disability Discrimination Act 1992*, the *Racial Discrimination Act 1975* or the *Sex Discrimination Act 1984*;

(i) in relation to ACIC—the compliance by that agency with:

(i) directions or guidelines given to that agency; or

(ii) policies or other decisions made;

by the Board of ACIC or the Inter-Governmental Committee established under the *Australian Crime Commission Act 2002*.

(3B) The functions of the Inspector-General under subsection (3A) do not include inquiring into any action taken by an examiner (within the meaning of the *Australian Crime Commission Act 2002*) of ACIC in performing functions or exercising powers as an examiner.

57 Subsection 8(5)

Omit "and (3)", substitute ", (3) and (3A)".

58 Subsection 8(5)

After "DIO", insert ", ACIC, the Australian Federal Police".

59 Paragraph 8A(1)(b)

Omit "intelligence agency", substitute "intelligence agency (within the meaning of this Act); and".

60 After paragraph 8A(1)(b)

Insert:

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

61 Subsection 8A(1)

After "so relates", insert "as described in paragraph (b)".

62 Paragraph 9AA(b)

Omit "paragraph 8(1)(d)", substitute "paragraphs 8(1)(d) and (3A)(b)".

63 After paragraph 9AA(b)

Insert:

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

64 Section 9A

Before "The functions", insert "(1)".

65 At the end of section 9A

Add:

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

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

(a) may, at all reasonable times, enter and remain on any premises (including any land or place); and

(b) is entitled to all reasonable facilities and assistance that the head of the agency is capable of providing; and

(c) is entitled to full and free access at all reasonable times to any information, documents or other property of the agency; and

(d) may examine, make copies of or take extracts from any information or documents.

66 At the end of subsection 10(1)

Add:

Note 1: A complaint is taken to have been made under this Act if all or part of the complaint is transferred to the Inspector-General by an integrity body (see section 32AE of this Act).

Note 2: See also Part IIIA which deals with relationships with other agencies and information sharing.

67 Before subsection 11(2)

Insert:

When inquiry or further inquiry into complaints is not required

68 After subsection 11(4)

Insert:

(4A) Without limiting paragraph (2)(c), the Inspector-General may decide not to inquire into, or not to inquire further into, a complaint or part of a complaint in relation to action taken by an intelligence agency if:

(a) a complaint in respect of the action has been, or could have been, made by the complainant to any of the following persons or bodies (the ***integrity body*** for the complaint):

(i) the Ombudsman;

(ii) the Australian Human Rights Commission, under Division 3 of Part II (human rights complaints) or

Part IIB (unlawful discrimination complaints) of the *Australian Human Rights Commission Act 1986*;

(iii) the Information Commissioner under Part V of the *Privacy Act 1988*;

(iv) the Integrity Commissioner;

(v) the Inspector-General ADF; and

(b) the Inspector-General is satisfied that the subject matter of the complaint or the part of the complaint could be more effectively or conveniently dealt with by the integrity body for the complaint.

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

Inquiries into complaints about employment, contracts and related matters

69 Paragraph 15(3)(a)

After "ASD" (wherever occurring), insert ", ACIC, the Australian Federal Police".

70 Paragraph 21(1B)(a)

After "ASD" (wherever occurring), insert ", ACIC, the Australian Federal Police".

71 After Part III

Insert:

Part IIIA—Relationships with other agencies and information sharing

32AC Information sharing with integrity bodies

(1) The Inspector-General may share information or documents with an integrity body (the ***receiving body***) if:

(a) the information or documents are obtained by the Inspector-General in the course of exercising powers, or

performing functions or duties, in relation to ACIC or the Australian Federal Police; and

(b) the information or documents are relevant to the receiving body's functions; and

(c) the Inspector-General is satisfied on reasonable grounds that the receiving body has satisfactory arrangements in place for protecting the information or documents.

(2) To avoid doubt, the Inspector-General may share information or documents with an integrity body whether or not the Inspector-General is transferring a complaint or part of a complaint to the integrity body.

(3) Without limiting paragraph (1)(c), the Inspector-General may make arrangements with the head of an intelligence agency in relation to protecting information or documents provided to the Inspector-General by the agency.

32AD Transferring complaints to other integrity bodies

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

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

32AE Complaints transferred by integrity bodies

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

Note: Complaints may be transferred to the Inspector-General under subsections 20(4C) of the *Australian Human Rights Commission Act 1986*, 6F(3) of the *Ombudsman Act 1976* and 50(3) of the *Privacy Act 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

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

75 Subsections 32B(2) and (4)

Repeal the subsections, substitute:

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

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

(b) that are given:

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

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

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

(a) the Minister; or

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

76 After section 34B

Insert:

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

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

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

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

an IGIS official does not bear an evidential burden in relation to whether the disclosure, record or use is for the purposes of, or in connection with, that or any other IGIS official exercising a power, 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

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

(b) the complaint or the part of the complaint involves an allegation, or information, that raises a corruption issue;

the person who made the complaint is taken to have referred the allegation or information to the Integrity Commissioner under subsection 23(1).

80 After subsection 90(3A)

Insert:

Disclosure to IGIS officials

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

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

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

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

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

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

81 After paragraph 208(3)(a)

Insert:

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

82 Subsection 208(7)

After "or (6)", insert "(except to the Inspector-General of Intelligence and Security for the purpose of performing the Inspector-General's functions)".

83 At the end of section 208

Add:

Notifying the Attorney-General

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

Ombudsman Act 1976

84 Subsection 3(1)

Insert:

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

85 After section 5A

Insert:

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

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

(a) ACC (except action taken by an examiner of ACC performing functions or exercising powers as an examiner); or

(b) the Australian Federal Police;

if the Inspector-General of Intelligence and Security transfers all or part of the complaint to the Ombudsman under section 32AD of 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:

(a) must consult the Inspector-General of Intelligence and Security about the complaint or the part of the complaint that relates to the action; and

(b) may decide not to investigate the action, or not to continue to investigate the action.

Transfer to Inspector-General of Intelligence and Security

(3) If the Ombudsman decides not to investigate, or not to continue to investigate, an action under paragraph (2)(b), and the Inspector-General of Intelligence and Security agrees to the transfer of the complaint or the part of the complaint, the Ombudsman must:

(a) transfer the complaint or part to the Inspector-General of Intelligence and Security; and

(b) as soon as is reasonably practicable, take reasonable steps to give the complainant written notice that the complaint or part has been transferred; and

(c) give the Inspector-General of Intelligence and Security any information or documents relating to the complaint or part that are in the possession, or under the control, of the Ombudsman.

Relationship with other provisions

(4) This section does not limit the power of the Ombudsman to transfer a complaint or part of a complaint to the Inspector-General of Intelligence and Security under another provision of this Act or any other Act.

(5) Subsection 35(2) does not prevent the Ombudsman, or an officer acting on behalf of the Ombudsman, from giving information or documents under paragraph (3)(c) of this section.

89 At the end of subsection 35(6)

Add:

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

90 After section 35AA

Insert:

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

(1) This section applies if:

(a) either:

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

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

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

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

(a) disclosing the information; or

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

(c) giving the document;

to the Inspector-General.

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

Add ", except to the Inspector-General of Intelligence and Security in accordance with section 35AB".

Privacy Act 1988

92 After section 49A

Insert:

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

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

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

Insert:

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

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

Insert:

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

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

Insert:

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

Public Interest Disclosure Act 2013

96 Section 8

Insert:

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

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

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

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

Insert:

(ca) if the discloser believes on reasonable grounds that:
(i) the disclosure relates to action taken by ACIC or the Australian Federal Police in relation to that agency's intelligence functions; and
(ii) it would be appropriate for the disclosure to be investigated by the IGIS;
the IGIS;

98 Section 42 (note 2)

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

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

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

100 After subsection 43(3)

Insert:

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

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

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

102 Section 46 (note)

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

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

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:

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

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

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

Omit "or a record of data disruption intercept information", substitute ", a record of data disruption intercept information or a record of network activity warrant intercept information".

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

After "data disruption warrant", insert ", a network activity warrant".

115 Paragraph 7(2)(bb)

Omit "or 27KE(9)", substitute ", 27KE(9) or 27KP(8)".

116 After section 63AD

Insert:

63AE Dealing in network activity warrant intercept information etc.

(1) A person may, for the purposes of doing a thing authorised by a network activity warrant:

(a) communicate network activity warrant intercept information to another person; or

(b) make use of network activity warrant intercept information; or

(c) make a record of network activity warrant intercept information; or

(d) give network activity warrant intercept information in evidence in:

(i) a criminal proceeding for an offence against section 105 so far as the offence relates to contravening section 63; or

(ii) a proceeding that is not a criminal proceeding.

(2) A person may:

(a) communicate network activity warrant intercept information to another person; or

(b) make use of network activity warrant intercept information; or

(c) make a record of network activity warrant 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;

(e) acting for, or on behalf of, a foreign power (within the meaning of the *Australian Security Intelligence Organisation Act 1979*);

(f) activities that are, or are likely to be, a threat to security;

(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);

(h) activities that pose a risk, or are likely to pose a risk, to the operational security (within the ordinary meaning of that expression) of the Organisation or of AGO or ASD (within the meanings of the *Intelligence Services Act 2001*);

(i) activities related to the proliferation of weapons of mass destruction or the movement of goods listed from time to time in the Defence and Strategic Goods List (within the meaning of regulation 13E of the *Customs (Prohibited Exports) Regulations 1958*);

(j) activities related to a contravention, or an alleged contravention, by a person of a UN sanction enforcement law (within the meaning of the *Charter of the United Nations Act 1945*).

(3) A person may, in connection with:

(a) the performance by an IGIS official of the IGIS official's functions or duties; or

(b) the exercise by an IGIS official of the IGIS official's powers;

communicate to the IGIS official, or make use of, or make a record of, network activity warrant intercept information.

(4) An IGIS official may, in connection with:

(a) the performance by the IGIS official of the IGIS official's functions or duties; or

(b) the exercise by the IGIS official of the IGIS official's powers;

communicate to another person, or make use of, or make a record of, network activity warrant intercept information.

(5) If:

(a) information was obtained by intercepting a communication passing over a telecommunications system; and

(b) the interception was purportedly for the purposes of doing a thing specified in a network activity warrant; and

(c) the interception was not authorised by the network activity warrant;

then:

(d) a person may, in connection with:

(i) the performance by an IGIS official of the IGIS official's functions or duties; or

(ii) the exercise by an IGIS official of the IGIS official's powers;

communicate to the IGIS official, or make use of, or make a record of, that information; and

(e) an IGIS official may, in connection with:

(i) the performance by the IGIS official of the IGIS official's functions or duties; or

(ii) the exercise by the IGIS official of the IGIS official's powers;

communicate to another person, or make use of, or make a record of, that information.

(6) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution for an offence against section 63 of this Act, an IGIS official does not bear an evidential burden in relation to the matters in subsection (4) or (5) of this section.

117 Paragraph 67(1)(a)

Omit "or data disruption intercept information", substitute ", data disruption intercept information or network activity warrant intercept information".

118 Section 68

Omit "or data disruption intercept information", substitute ", data disruption intercept information or network activity warrant intercept information".

119 Subsection 74(1)

After "data disruption intercept information", insert ", network activity warrant intercept information".

120 Subsection 75(1)

After "data disruption warrant", insert ", a network activity warrant".

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

After "63AD,", insert "63AE,".

122 After paragraph 108(2)(cc)

Insert:

(cd) accessing a stored communication under a network activity 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.

- 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:

(a) the Australian Federal Police and the ACC; and
(b) law enforcement officers.

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.

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

computer means all or part of:

(a) one or more computers; or

(b) one or more computer systems; or

(c) one or more computer networks; or

(d) any combination of the above.

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

emergency authorisation means an emergency authorisation given under section 3ZZUX.

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

(a) the law enforcement officer named in the warrant by the issuing magistrate as being responsible for executing the warrant; or

(b) if that law enforcement officer does not intend to execute the warrant—another law enforcement officer whose name has been written in the warrant by the law enforcement officer so named; or

(c) another law enforcement officer whose name has been written in the warrant by the law enforcement officer last named in the warrant.

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

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*.

law enforcement agency means:

(a) the Australian Federal Police; or

(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.

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

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

takes control has the meaning given by section 3ZZUL.

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

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

3ZZUL When a person takes control of an online account

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

(2) The following are examples of such steps:

(a) using existing account credentials to alter one or more account credentials;

(b) removing a requirement for two-factor authentication;

(c) altering the kind or kinds of account credentials that are required to access or operate the account.

3ZZUM Appropriate authorising officer

Australian Federal Police

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

(a) the chief officer of the Australian Federal Police; or

(b) a Deputy Commissioner of the Australian Federal Police; or

(c) a senior executive AFP employee who is authorised under subsection (2).

(2) The chief officer of the Australian Federal Police may authorise, in writing, a person who is a senior executive AFP employee to be an appropriate authorising officer of the Australian Federal Police for 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:

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

Unsworn applications

(2B) If a law enforcement officer believes that:
(a) taking control of the target accounts is immediately necessary, in the course of the investigation mentioned in paragraph (1)(c), for the purpose of enabling evidence to be obtained of the commission of the offences mentioned in that paragraph; and
(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made;
an application for an account takeover warrant under subsection (1) may be made before an affidavit is prepared or sworn.

(2C) If subsection (2B) applies, the applicant must:
(a) provide as much information as the magistrate 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 magistrate, whether or not a warrant has been issued.

(2D) If:
(a) subsection (2B) applies; and
(b) transmission by fax is available; and
(c) an affidavit has been prepared;
the person applying must transmit a copy of the affidavit, whether sworn or unsworn, to the magistrate who is to determine the application.

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

(4) A magistrate may require an applicant to provide such additional information as is necessary for the proper consideration of the application.

(5) As soon as practicable after making an urgent application that was not made in writing, the applicant must:

(a) make a written record of the application; and

(b) give a copy of the record to the magistrate to whom the application was made.

3ZZUP Determining the application

(1) A magistrate may issue an account takeover warrant if satisfied that there are reasonable grounds for the suspicion founding the application for the warrant.

(2) In determining whether an account takeover warrant should be issued, the magistrate must have regard to:

(a) the nature and gravity of the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is sought; and

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

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

(d) the likely evidentiary value of any evidence sought to be obtained; and

(da) the extent to which the execution of the warrant is likely to impact on persons lawfully using a computer, so far as that matter is known to the magistrate; and

(db) the extent to which the execution of the warrant is likely to cause a person to suffer a temporary loss of:

(i) money; or

(ii) digital currency; or

(iii) property (other than data);

so far as that matter is known to the magistrate; and

(dc) if:

(i) the magistrate believes on reasonable grounds that each target account is held by a person who is working in a

professional capacity as a journalist or of an employer of such a person; and

(ii) the alleged relevant offence, or each of the alleged relevant offences, in respect of which the warrant is sought is an offence against a secrecy provision;

whether the public interest in issuing the warrant outweighs:

(iii) the public interest in protecting the confidentiality of the identity of the journalist's source; and

(iv) the public interest in facilitating the exchange of information between journalists and members of the public so as to facilitate reporting of matters in the public interest; and

(e) any previous warrant sought or issued under this Division in connection with the same online account; and

(f) any previous warrant sought or issued under this Division in connection with the same alleged relevant offence or the same alleged relevant offences.

(3) For the purposes of having regard to the nature and gravity of the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is sought, the magistrate must give weight to the following matters:

(a) whether the conduct constituting the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is sought amounts to:

(i) an activity against the security of the Commonwealth; or

(ii) an offence against Chapter 5 of the *Criminal Code*;

(b) whether the conduct constituting the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is sought amounts to:

(i) an activity against the proper administration of Government; or

(ii) an offence against Chapter 7 of the *Criminal Code*;

(c) whether the conduct constituting the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is sought:

(i) causes, or has the potential to cause, serious violence, or serious harm, to a person; or

(ii) amounts to an offence against Chapter 8 of the *Criminal Code*;

(d) whether the conduct constituting the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is sought:

(i) causes, or has the potential to cause, a danger to the community; or

(ii) amounts to an offence against Chapter 9 of the *Criminal Code*;

(e) whether the conduct constituting the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is sought:

(i) causes, or has the potential to cause, substantial damage to, or loss of, data, property or critical infrastructure; or

(ii) amounts to an offence against Chapter 10 of the *Criminal Code*;

(f) whether the conduct constituting the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is sought involves, or is related to, the commission of:

(i) transnational crime; or

(ii) serious crime; or

(iii) organised crime;

that is not covered by any of the preceding paragraphs.

(4) Subsection (3) does not limit the matters that may be considered by the magistrate.

(5) To avoid doubt, this Act does not prevent an account takeover warrant from being issued in a case where the conduct constituting the alleged relevant offence, or alleged relevant offences, in respect of which the warrant is sought 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.

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:

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

(ii) is covered by the warrant;

(f) copying any account credentials to which the target account relates;

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

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

(a) access has been obtained to account-based data; and

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

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

When account-based data is covered by a warrant

(4) For the purposes of this section, account-based data is ***covered by*** a warrant if access to the data 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.

Certain acts not authorised

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

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

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

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

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

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

(d) it is not practicable in the circumstances to apply for an account takeover warrant.

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

(3) The appropriate authorising officer may give the emergency authorisation if satisfied that there are reasonable grounds for the suspicion founding the application.

Statutory conditions

(4) An emergency authorisation is subject to the following conditions:

(a) the authorisation must not be executed in a manner that results in damage to data unless the damage is justified and proportionate, having regard to the risk of serious violence or substantial damage referred to in paragraph (1)(a);

(b) the authorisation must not be executed in a manner that causes a person to suffer a permanent loss of:

(i) money; or

(ii) digital currency; or

(iii) property (other than data).

3ZZUY Record of emergency authorisations to be made

As soon as practicable after an appropriate authorising officer gives an emergency authorisation, the officer must make a written record of the giving of that authorisation, including in the record:

(a) the name of the applicant for the authorisation; and

(b) the date and time the authorisation was given; and

(c) the nature of the authorisation given.

3ZZUZ Attributes of emergency authorisations

(1) An emergency authorisation may authorise anything that an account takeover warrant may authorise.

(2) A law enforcement officer may take control of an online account under an emergency authorisation only if the officer is acting in the 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

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

Grant of assistance order

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

(a) there are reasonable grounds for suspecting that taking control of the account is necessary, in the course of the investigation to which the account takeover warrant relates, 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; and

(b) the specified person is:

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

(ii) the holder of the account; or

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

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

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

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

(c) the specified person has relevant knowledge of:

(i) the account; or

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

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

(2A) In determining whether the assistance order should be granted, the magistrate 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 3LA of this Act; or

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

so far as that matter is known to the magistrate.

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

Duration of assistance order

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

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

Protection from civil liability

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

(a) in compliance with an assistance order; or

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

Offence

(3) A person commits an offence if:

(a) the person is subject to an order under this section; and

(b) the person is capable of complying with a requirement in the order; and

(c) the person omits to do an act; and

(d) the omission contravenes the requirement.

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

Additional use of information etc.

(4) If information or assistance is provided under this section in connection with an investigation into one or more alleged relevant offences, this Act does not, by implication, prevent the information or assistance from being used in connection with the execution of a 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

(g) for the purposes of obtaining legal advice in relation to this Part; or

(h) in accordance with any requirement imposed by law; or

(i) in connection with the performance of functions or duties, or the exercise of powers, under this Part; or

(j) in connection with the performance of functions or duties, or the exercise of powers, by:

(i) a law enforcement officer; or

(ii) the Director-General (within the meaning of the *Australian Security Intelligence Organisation Act 1979*), an ASIO employee (within the meaning of that Act) or an ASIO affiliate (within the meaning of that Act); or

(iii) the agency head (within the meaning of the *Intelligence Services Act 2001*), or a staff member (within the meaning of that Act), of an agency (within the meaning of that Act); or

(k) for the purposes of the admission of evidence in a proceeding that is not a criminal proceeding.

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

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

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

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

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

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

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

(a) must ensure that every record or report comprising protected information is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report; and

(b) must cause to be destroyed any record or report referred to in paragraph (a):

(i) as soon as practicable after the making of the record or report if the chief officer is satisfied that no civil or criminal proceeding to which the material contained in the record or report relates has been, or is likely to be, commenced and that the material contained in the record or report is not likely to be required in connection with an activity or purpose referred to in subsection 3ZZVH(2), (3) or (4); and

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

3ZZVK Protection of account takeover 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 account takeover 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 account takeover 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:

account takeover technologies or methods means:

(a) technologies or methods relating to the use of:

(i) a computer; or

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

(iii) any other electronic equipment; or

(iv) a data storage device;

for the purpose of taking control of an online account; or

(b) technologies or methods relating to adding, copying, deleting or altering account-based data, if doing so is necessary to achieve the purpose mentioned in paragraph (a); or

(c) technologies or methods relating to adding, copying, deleting or altering account credentials to which an online account relates, if doing so is necessary to achieve the purpose mentioned in paragraph (a);

where the technologies or methods have been, or are being, deployed in giving effect to an account takeover warrant or emergency authorisation.

proceeding includes a proceeding before a court, tribunal or Royal 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

(ii) the dates on which those refusals occurred; and

(l) if one or more applications for approval of the giving of emergency authorisations were made by or on behalf of appropriate authorising 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

(m) if the giving of one or more emergency authorisations were approved during the previous 12 months in response to applications made by or on behalf of appropriate authorising officers of the Australian Federal Police or the ACC, as the case requires:

(i) the number of those approvals; and

(ii) the dates on which those approvals were given; and

(n) if one or more applications for approval of the giving of emergency authorisations made by or on behalf of appropriate authorising 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.

(2) The following information is listed for the purposes of subparagraph (1)(h)(vi):

(a) the name of the executing officer;

(b) the names of any other law enforcement officers involved in executing the warrant;

(c) the period during which the warrant was executed;

(d) the target account;

(e) if the holder of the target account is known to the executing officer—the holder;

(f) if one or more users of the target account (other than the holder of the target account) are known to the executing officer—those users;

(g) details of the benefit of the execution of the warrant to the investigation of a relevant offence;

(h) details of how information obtained under the warrant was used;

(i) details of the communication of information obtained under the warrant to persons other than:

(i) if the warrant was issued in response to an application made by a law enforcement officer of the Australian Federal Police—law enforcement officers of the Australian Federal Police; or

(ii) if the warrant was issued in response to an application made by a law enforcement officer of the ACC—law enforcement officers of the ACC;

(j) details of the compliance with the conditions (if any) to which the warrant was subject.

(3) For the purposes of paragraph (2)(d), the target account may be specified by identifying one or more matters and things that are sufficient to identify the account.

3ZZVM Chief officers' annual reports to the Minister

(1) As soon as practicable, and in any event within 3 months, after the end of each financial year, the chief officer of the Australian Federal Police or the ACC must submit a report to the Minister 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 financial year; and

(b) the number of account takeover warrants issued during the financial year in response to applications made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires; 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 financial year were refused—the number of those refusals; and

(d) the number of urgent applications for account takeover warrants made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires, during the financial year; and

(e) the number of account takeover warrants issued during the financial year in response to urgent applications made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires; and

(f) if one or more urgent applications for account takeover warrants made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires, during the financial year were refused—the number of those refusals; and

(g) if one or more variations of account takeover warrants were granted during the financial year in response to applications made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires—the number of those variations; and

(h) 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 financial year were refused—the number of those refusals; 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 financial year; and

(j) the number of emergency authorisations given during the financial year in response to applications made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires; 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 financial year were refused—the number of those refusals; and

(l) if one or more applications for approval of the giving of emergency authorisations were made by or on behalf of appropriate authorising officers of the Australian Federal Police or the ACC, as the case requires, during the financial year—the number of those applications; and

(m) if the giving of one or more emergency authorisations were approved during the financial year in response to applications made by or on behalf of appropriate authorising officers of

the Australian Federal Police or the ACC, as the case requires—the number of those approvals; and

(n) if one or more applications for approval of the giving of emergency authorisations made by or on behalf of appropriate authorising officers of the Australian Federal Police or the ACC, as the case requires, during the financial year were refused—the number of those refusals; and

(o) the types of relevant offences in respect of which account takeover warrants or emergency authorisations were sought by law enforcement officers of the Australian Federal Police or the ACC, as the case requires, during the financial year; and

(p) the number of arrests that were made during the financial year on the basis (wholly or partly) of information obtained under account takeover warrants issued, or emergency authorisations given, in response to applications made by law enforcement officers of the Australian Federal Police or the ACC, as the case requires; and

(q) the number of prosecutions for relevant offences that were commenced during the financial year in which information obtained under account takeover warrants or emergency authorisations was given in evidence, and the number of those prosecutions in which a person was found guilty.

(2) The Minister must cause a copy of the report to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives it.

(3) A copy of a report given to the Minister under this section must be given to the Ombudsman at the same time as it is given to the Minister.

3ZZVN Keeping documents connected with account takeover warrants

The chief officer of the Australian Federal Police or the ACC must cause the following to be kept:

(a) a copy of each application for an account takeover warrant that was made by a law enforcement officer of the Australian Federal Police or the ACC, as the case requires;

(b) a copy of each account takeover warrant that was issued in response to an application made by a law enforcement officer of the Australian Federal Police or the ACC, as the case requires;

(c) each written application for an emergency authorisation made by a law enforcement officer of the Australian Federal Police or the ACC, as the case requires;

(d) a copy of each emergency authorisation that was given in response to an application made by a law enforcement officer of the Australian Federal Police or the ACC, as the case requires;

(e) a copy of each application made by or on behalf of an appropriate authorising officer for approval of the giving of an emergency authorisation to a law enforcement officer of the Australian Federal Police or the ACC, as the case requires;

(f) a copy of each section 3ZZVG assistance order that was made in response to an application made by a law enforcement officer of the Australian Federal Police or the ACC, as the case requires;

(g) a copy of each application for a section 3ZZVG assistance order that was made by a law enforcement officer of the Australian Federal Police or the ACC, as the case requires;

(h) if an application for a variation of an account takeover warrant was made by a law enforcement officer of the Australian Federal Police or the ACC, as the case requires—a copy of the application;

(i) if an account takeover warrant that was varied in response to an application made by a law enforcement officer of the Australian Federal Police or the ACC, as the case requires—a copy of the variation;

(j) if an account takeover warrant issued in response to an application made by a law enforcement officer of the Australian Federal Police or the ACC, as the case requires, was revoked—a copy of the revocation;

(k) each written record made under subsection 3ZZUN(5);

(l) a copy of each report given to the Minister and the 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:

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

(ii) the alleged relevant offence, or alleged relevant offences, in respect of which the authorisation was given; and

(iii) the date on which the application for approval of the giving of the authorisation was made; and

(iv) whether that application for approval of the giving of the authorisation was successful or not.

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

Division 7—Inspections

3ZZVQ Appointment of inspecting officers

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

3ZZVR Inspection of records by the Ombudsman

(1) The Ombudsman must, from time to time and at least once every 12 months, inspect the records of the Australian Federal Police and the ACC to determine the extent of compliance with this Part by:

(a) the Australian Federal Police or the ACC, as the case requires; and

(b) law enforcement officers of the Australian Federal Police or the ACC, as the case requires.

(2) For the purpose of an inspection under this section, the Ombudsman:

(a) may, after notifying the chief officer of the Australian Federal Police or the ACC, enter at any reasonable time premises occupied by the Australian Federal Police or the ACC, as the case requires; and

(b) is entitled to have full and free access at all reasonable times to all records of the Australian Federal Police or the ACC that are relevant to the inspection; and

(c) may require a member of staff of the Australian Federal Police or the ACC to give the Ombudsman any information that the Ombudsman considers necessary, so long as:

(i) the information is in the member's possession, or the member has access to the information; and

(ii) the information is relevant to the inspection; and

(d) may, despite any other law, make copies of, and take extracts from, records of the Australian Federal Police or the ACC.

(3) The chief officer of the Australian Federal Police or the ACC must ensure that members of staff of the Australian Federal Police or the ACC, as the case requires, give the Ombudsman any assistance the Ombudsman reasonably requires to enable the Ombudsman to perform functions under this section.

3ZZVS Power to obtain relevant information

(1) If the Ombudsman has reasonable grounds to believe that a law enforcement officer of the Australian Federal Police or the ACC is able to give information relevant to an inspection under this Division of the records of the Australian Federal Police or the ACC, subsections (2) and (3) have effect.

(2) The Ombudsman may, by writing given to the law enforcement officer, require the officer to give the information to the Ombudsman:

(a) by writing signed by the officer; and

(b) at a specified place and within a specified period.

(3) The Ombudsman may, by writing given to the law enforcement officer, require the officer to attend:

(a) before a specified inspecting officer; and

(b) at a specified place; and

(c) within a specified period or at a specified time on a specified day;

to answer questions relevant to the inspection.

(4) If the Ombudsman:

(a) has reasonable grounds to believe that a law enforcement officer of the Australian Federal Police or the ACC is able to

give information relevant to an inspection under this Division of the records of the Australian Federal Police or the ACC; and

(b) does not know the officer's identity;

the Ombudsman may, by writing given to the chief officer of the Australian Federal Police or the ACC, as the case requires, require the chief officer, or a person nominated by the chief officer, to attend:

(c) before a specified inspecting officer; and

(d) at a specified place; and

(e) within a specified period or at a specified time on a specified day;

to answer questions relevant to the inspection.

(5) The place, and the period or the time and day, specified in a requirement under this section, must be reasonable having regard to the circumstances in which the requirement is made.

3ZZVT Offence

A person commits an offence if:

(a) the person is required under section 3ZZVS to attend before an inspecting officer, to give information or to answer questions; and

(b) the person refuses or fails to do so.

Penalty: Imprisonment for 6 months.

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

(1) Despite any other law, a person is not excused from giving information, answering a question, or giving access to a document, as and when required under this Division, on the ground that giving the information, answering the question, or giving access to the document, as the case may be:

(a) would contravene a law; or

(b) would be contrary to the public interest; or

(c) might tend to incriminate the person; or

(d) would disclose one of the following:

(i) a legal advice given to a Minister, a Department or a prescribed authority;

(ii) a communication between an officer of a Department or of a prescribed authority and another person or body, being a communication protected against disclosure by legal professional privilege.

(2) However, if the person is an individual:

(a) the information, the answer, or the fact that the person has given access to the document, as the case may be; and

(b) any information or thing (including a document) obtained as a direct or indirect consequence of giving the information, answering the question or giving access to the document;

is not admissible in evidence against the person except in a proceeding by way of a prosecution for an offence against section 3ZZVH of this Act or Part 7.4 or 7.7 of the *Criminal Code*.

(3) If, at general law, an individual would otherwise be able to claim the privilege against self-exposure to a penalty (other than a penalty for an offence) in relation to giving information, answering a question, or giving access to a document, as and when required under this Division, the individual is not excused from giving the information, answering the question, or giving access to the document, as the case may be, on that ground.

Note: A body corporate is not entitled to claim the privilege against self-exposure to a penalty.

(4) Nothing in section 3ZZVH or in any other law prevents a law enforcement officer of the Australian Federal Police or the ACC from:

(a) giving information to an inspecting officer (whether orally or in writing and whether or not in answer to a question); or

(b) giving access to a record of the Australian Federal Police or the ACC, as the case requires, to an inspecting officer;

for the purposes of an inspection under this Division of the records of the Australian Federal Police or the ACC, as the case requires.

(5) Nothing in section 3ZZVH or in any other law prevents a law enforcement officer from making a record of information, or causing a record of information to be made, for the purposes of giving the information to a person as permitted by subsection (4).

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

(7) In this section:

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

3ZZVV Delegation by Ombudsman

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

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

3ZZVW Ombudsman not to be sued

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

3ZZVX Report on inspection

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

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

(a) prejudice an investigation or prosecution; or

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

(3) The Minister must cause a copy of the report to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives the report.

Division 8—Miscellaneous

3ZZVY Minor defects in connection with account takeover warrant

(1) If:

(a) information is purportedly obtained under an account takeover warrant; and

(b) there is a defect or irregularity in relation to the warrant; and

(c) but for that defect or irregularity, the warrant would be a sufficient authority for obtaining the information;

then:

(d) obtaining the information is taken to be as valid; and

(e) the information obtained may be dealt with, or given in evidence in any proceeding;

as if the warrant did not have that defect or irregularity.

(2) A reference in subsection (1) to a defect or irregularity in relation to the warrant is a reference to a defect or irregularity (other than a substantial defect or irregularity):

(a) in, or in connection with the issue of, a document purporting to be that warrant; or

(b) in connection with the execution of that warrant or the purported execution of a document purporting to be that warrant.

3ZZVZ Evidentiary certificates

(1) A law enforcement officer may issue a written certificate signed by the officer setting out any facts the officer considers relevant with respect to:

(a) anything done by the law enforcement officer, or by a person assisting or providing technical expertise to the law

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

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

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

(ii) the making use of; or

(iii) the making of a record of; or

(iv) the custody of a record of;

information obtained under an account takeover warrant.

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

3ZZWA Compensation for property loss or serious damage

(1) If a person suffers:

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

(b) personal injury;

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

(c) the Federal Court of Australia; or

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

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

National Emergency Declaration Act 2020

5 Paragraph 15(8)(a)

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);

(ga) activities that pose a risk, or are likely to pose a risk, to the operational security (within the ordinary meaning of that expression) of the Organisation or of AGO or ASD (within the meanings of the *Intelligence Services Act 2001*);

8 Paragraph 63AC(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);

(ga) activities that pose a risk, or are likely to pose a risk, to the operational security (within the ordinary meaning of that expression) of the Organisation or of AGO or ASD (within the meanings of the *Intelligence Services Act 2001*);