Dedicated Encrypted Criminal Communication Device Prohibition Orders Act 2022 No 46

[2022-46]

New South Wales

Status Information

Currency of version

Historical version for 18 October 2022 to 1 February 2023 (accessed 22 November 2024 at 10:21)

Legislation on this site is usually updated within 3 working days after a change to the legislation.

Provisions in force

The provisions displayed in this version of the legislation have all commenced.

Notes—

- **Note**
  Amending provisions are subject to automatic repeal pursuant to sec 30C of the *Interpretation Act 1987 No 15* once the amendments have taken effect.

Authorisation

This version of the legislation is compiled and maintained in a database of legislation by the Parliamentary Counsel's Office and published on the NSW legislation website, and is certified as the form of that legislation that is correct under section 45C of the Interpretation Act 1987.

File last modified 1 February 2023

Dedicated Encrypted Criminal Communication Device Prohibition Orders Act 2022 No 46

New South Wales

Contents

Dedicated Encrypted Criminal Communication Device Prohibition Orders Act 2022 No 46

New South Wales

An Act to establish a scheme for dedicated encrypted criminal communication device prohibition orders; to create a new offence in the *Crimes Act 1900* in relation to possessing a dedicated encrypted criminal communication device to commit or facilitate serious criminal activity; and to make consequential amendments to other legislation.

Part 1 Preliminary

1 Name of Act

This Act is the *Dedicated Encrypted Criminal Communication Device Prohibition Orders Act 2022*.

2 Commencement

This Act commences on 1 February 2023.

3 Definitions

The Dictionary in Schedule 1 defines words and expressions used in this Act.

Note—

The *Interpretation Act 1987* also contains definitions and other provisions that affect the interpretation and application of this Act.

Part 2 Powers given by dedicated encrypted criminal communication device prohibition orders

4 Purpose of dedicated encrypted criminal communication device prohibition orders

The purpose of a dedicated encrypted criminal communication device prohibition order is to provide an investigative tool for police investigating the involvement of the subject of the order in criminal activity involving dedicated encrypted criminal communication devices.

5 Entry and search powers under dedicated encrypted criminal communication device

prohibition orders

(1) If a dedicated encrypted criminal communication device prohibition order is in force against a person, a police officer may, without a warrant, do one or more of the following for the purpose of determining whether the person is in possession of a dedicated encrypted criminal communication device—

(a) stop, detain and search the person but not another person,

(b) enter and search the following premises (***searchable premises***)—

(i) premises at which the person resides,

(ii) premises the police officer reasonably suspects are owned by the person or under the direct control or management of the person,

(iii) premises the police officer reasonably suspects are being used by the person for an unlawful purpose,

(c) stop, detain and search a vehicle—

(i) being driven by or otherwise under the control or management of the person or occupied by the person, or

(ii) parked on an area that is part of, or provided for the use of, searchable premises, but not if the area is shared with another dwelling or other premises, or

(iii) parked on an area that is part of, or provided for the use of, searchable premises and that is shared with another dwelling or other premises, but only if the police officer reasonably suspects that the vehicle is being used by the person for an unlawful purpose,

(d) give a direction under section 6,

(e) use electronic equipment to inspect or search a computer identified during a search conducted under paragraph (a)–(c).

(2) The *Law Enforcement (Powers and Responsibilities) Act 2002* applies to a search carried out under this Act.

Note—

See that Act, section 32 and Part 15 for additional limitations on the exercise of the powers under this section.

(3) Despite subsection (2), a strip search of a person must not be carried out when exercising a power under this section unless it is authorised under the *Law Enforcement (Powers and Responsibilities) Act 2002*, Part 4, Division 4.

6 Power to give directions

(1) For section 5(1)(d), a police officer exercising a power under section 5 may give a direction to a person against whom a dedicated encrypted criminal communication device prohibition order is in force to give a police officer information or assistance that is reasonable and necessary to view, or enable access to, data held in or accessible from—

(a) a computer identified during the search that the police officer has reasonable grounds to suspect is a dedicated encrypted criminal communication device, or

(b) a computer seized under the dedicated encrypted criminal communication device prohibition order that the police officer has reasonable grounds to suspect is a dedicated encrypted criminal communication device.

(2) A person given a direction under subsection (1)(a) or (b) must not, without reasonable excuse, fail to comply with the direction.

Maximum penalty—Imprisonment for 3 years.

(3) Without limiting subsection (2), it is not a reasonable excuse for a person given a direction under subsection (1)(a) or (b) to fail to comply with the direction on the ground that complying with the direction or the requirement would tend to incriminate the person or otherwise expose the person to a penalty.

7 Seizure etc powers under dedicated encrypted criminal communication device prohibition orders

A police officer may, in the exercise of powers under section 5, seize and detain all or part of a thing the police officer suspects on reasonable grounds—

(a) may provide evidence of the commission of an offence involving a dedicated encrypted criminal communication device, or

(b) is stolen or otherwise unlawfully obtained, or

(c) may provide evidence of the commission of a relevant offence within the meaning of the *Law Enforcement (Powers and Responsibilities) Act 2002*, Part 4, Division 1, or

(d) is a dangerous article within the meaning of the *Law Enforcement (Powers and Responsibilities) Act 2002*.

8 Requirement to give notice about searches in certain circumstances

(1) The Commissioner of Police must ensure the subject of a dedicated encrypted criminal communication device prohibition order is given written notice about a search as soon as practicable after the search if—

(a) a police officer searches premises or a vehicle under the order, and

(b) the subject of the order is not present during the search.

(2) A notice under subsection (1) must specify—

(a) the date on which the search took place, and

(b) the address or other description of the premises or vehicle searched.

Part 3 Applications for dedicated encrypted criminal communication device prohibition orders

9 Application for prohibition order

(1) A police officer, or another person on the police officer's behalf, may apply to an authorised magistrate for a dedicated encrypted criminal communication device prohibition order to be made against an eligible person.

(2) The application may be made only if—

(a) the police officer reasonably believes the eligible person is likely to use a dedicated encrypted criminal communication device to avoid law enforcement detection of criminal activity, and

(b) the application has been approved by a senior police officer.

(3) The application must not be made within—

(a) 2 weeks after an authorised magistrate has refused to grant a previous application against the eligible person, unless it contains material evidence or information not included in the previous application, or

(b) 6 months after the revocation of a dedicated encrypted criminal communication device prohibition order against the eligible person.

10 Form and content of application

(1) An application for a dedicated encrypted criminal communication device prohibition order must be in the form of an affidavit that—

(a) states the identity of the eligible person, and

(b) if the eligible person has been convicted of serious criminal offences—sets out details of each of the convictions, and

(c) sets out the grounds on which the dedicated encrypted criminal communication device prohibition order is sought, and

(d) includes evidence that the eligible person is likely to use a dedicated encrypted criminal communication device to avoid law enforcement detection of criminal activity, and

(e) sets out details of any dedicated encrypted criminal communication device prohibition orders that have been made in relation to the eligible person, and

(f) states the identity of any other persons, so far as is reasonably practicably known, who may be adversely affected by the order, and

(g) includes any information known to the applicant that may be adverse to the application or, if no adverse information is known, a statement to that effect, and

(h) specifies the period for which the dedicated encrypted criminal communication device prohibition order is sought.

(2) The application must be accompanied by a document signed by a senior police officer authorising the applicant to seek the dedicated encrypted criminal communication device prohibition order against the eligible person.

11 Notice of application to oversight commissioner

(1) The Commissioner of Police must ensure the oversight commissioner is given a notice containing the information set out in—

(a) an application for a dedicated encrypted criminal communication device prohibition order, and

(b) the document that accompanies the application.

(2) The notice must be given as far in advance of the application being made as is reasonably practicable.

(3) After deciding the application, the authorised magistrate must ensure that the application and accompanying document and affidavit are forwarded to the oversight commissioner.

(4) The oversight commissioner must keep the application and accompanying document and affidavit in a way that ensures they are not accessible to anyone who is not authorised to have access to them.

Part 4 Making of dedicated encrypted criminal communication device prohibition orders

12 Dedicated encrypted criminal communication device prohibition order may be made by authorised magistrate

(1) An authorised magistrate may make a dedicated encrypted criminal communication device prohibition order against a person if the magistrate is satisfied the person—

(a) is an eligible person, and

(b) is likely to use a dedicated encrypted criminal communication device to avoid law

enforcement detection of criminal activity.

(2) The authorised magistrate—

(a) must not make a dedicated encrypted criminal communication device prohibition order unless satisfied the oversight commissioner has been given a reasonable opportunity to make a submission in relation to the making of the order, and

(b) may ask the oversight commissioner for advice on any matter relating to the application or the making of the order.

13 Matters to be taken into account by authorised magistrate

(1) The authorised magistrate may, in deciding whether a person is likely to use a dedicated encrypted criminal communication device to avoid law enforcement detection of criminal activity, take any matter into account the authorised magistrate considers relevant.

(2) Without limiting subsection (1), the authorised magistrate may consider the following—

(a) the potential risk to public safety presented by the eligible person,

(b) whether the person associates with persons who are suspected to be involved in serious criminal activity,

(c) criminal intelligence about the person's suspected involvement in serious criminal activity or drug-related crime,

(d) whether the person is a member of, or associates with, a criminal group within the meaning of the *Crimes Act 1900*, section 93S,

(e) information from registered sources,

(f) surveillance reports,

(g) whether the person has cash or assets that are significantly out of proportion to the person's income.

(3) In this section—

serious criminal activity has the same meaning as in the *Crimes (Criminal Organisations Control) Act 2012*.

14 Process for making dedicated encrypted criminal communication device prohibition orders

(1) The person who is to be the subject of the dedicated encrypted criminal communication device prohibition order—

(a) is not entitled to be told about the application, and

(b) is not permitted to make a submission.

(2) The application is not required to be decided in a courtroom.

(3) The authorised magistrate may question, or ask for additional information about an application from, a police officer with knowledge of the application or the oversight commissioner—

(a) at any time, and

(b) in any way the authorised magistrate considers appropriate, including by audio link or audio visual link.

(4) A dedicated encrypted criminal communication device prohibition order—

(a) must not be made against a person when sentencing the person for an offence, and

(b) must instead be the subject of a separate application made in accordance with this Act.

(5) In this section—

audio link means technology that enables continuous and contemporaneous audio communication between persons at different places, including telephones.

audio visual link means technology that enables continuous and contemporaneous audio and visual communication between persons at different places, including video conferencing.

15 Record of and reasons for making of dedicated encrypted criminal communication device prohibition orders

(1) If an authorised magistrate decides to make a dedicated encrypted criminal communication device prohibition order, the magistrate must make a record of—

(a) the reasons for making the order, and

(b) the evidence used to support the decision to make the order.

(2) Except as otherwise provided for in this Act, a person, including the subject of the order—

(a) is not entitled to know the reasons for the decision to make the order, and

(b) is not to be given access to, or provided with, a document or a copy of a document that formed part of the application.

16 Form of dedicated encrypted criminal communication device prohibition order

(1) A dedicated encrypted criminal communication device prohibition order must—

(a) if there is an approved form for the order—be in the approved form, and

(b) be signed by the authorised magistrate who made the order.

(2) A dedicated encrypted criminal communication device prohibition order must include the following information—

(a) the name of the subject of the order,

(b) the name of the authorised magistrate who made the order,

(c) the date on which the order was made,

(d) that the order has been made under this Act because the subject of the order has been found to be likely to use a dedicated encrypted criminal communication device to avoid law enforcement detection of criminal activity,

(e) the period for which the order is to remain in force,

(f) the effect of the order,

(g) the way in which the subject of the order may seek to have the order revoked.

17 Commencement and duration of dedicated encrypted criminal communication device prohibition order

(1) A dedicated encrypted criminal communication device prohibition order commences when it is made.

(2) No power may be exercised under a dedicated encrypted criminal communication device prohibition order before a copy of the order has been served—

(a) personally on the subject of the order, or

(b) in accordance with section 18.

(3) A dedicated encrypted criminal communication device prohibition order remains in force until the earlier of the following—

(a) the end of the period specified by the authorised magistrate as the period for the order,

(b) the end of the period specified by a magistrate deciding an application for revocation of the order,

(c) the order is revoked.

(4) For subsection (3)(a), the period must not be—

(a) less than 6 months, or

(b) more than 2 years.

(5) The Commissioner of Police must ensure a record is kept of the date on which a dedicated encrypted criminal communication device prohibition order is served on the subject of the order.

18 Substituted service

(1) This section applies if, after reasonable attempts have been made to serve a copy of a dedicated encrypted criminal communication device prohibition order personally on the subject of the order, the Commissioner of Police is satisfied it cannot practicably be served on the subject.

(2) A police officer may apply to an authorised magistrate for approval to serve the dedicated encrypted criminal communication device prohibition order in another way.

(3) The authorised magistrate may, by order, direct that a copy of the dedicated encrypted criminal communication device prohibition order be served in another way specified in the magistrate's order.

Example of other ways of serving dedicated encrypted criminal communication device prohibition order—

by email or other electronic communication

(4) The authorised magistrate may make an order under subsection (3) only if the magistrate is satisfied—

(a) reasonable attempts have been made to serve the copy of the order personally on the subject of the order, and

(b) an alternative way of service is likely to enable the notice of the making of the order and details of the order to be communicated to the subject, and

(c) it is appropriate for the purposes of the order for service of the copy of the order to occur in another way.

(5) An order made under subsection (3) may be subject to any conditions the authorised magistrate considers appropriate.

Part 5 Revocation of dedicated encrypted criminal communication device prohibition orders

19 Revocation of dedicated encrypted criminal communication device prohibition order on

application of subject

(1) The subject of a dedicated encrypted criminal communication device prohibition order may apply to the Local Court to have the order revoked.

(2) The Commissioner of Police is the respondent to the application.

(3) The Local Court may require the applicant to provide the Court with a copy of the dedicated encrypted criminal communication device prohibition order.

(4) The Local Court may—

(a) affirm the dedicated encrypted criminal communication device prohibition order, or

(b) vary the term of the order, or

(c) revoke the order.

(5) The Local Court may revoke the dedicated encrypted criminal communication device prohibition order only if satisfied—

(a) the order is unreasonably onerous in the circumstances, or

(b) the subject of the order is not likely to use a dedicated encrypted criminal communication device to avoid law enforcement detection of criminal activity, or

(c) the risk of the subject of the order using a dedicated encrypted criminal communication device to avoid law enforcement detection of criminal activity could be mitigated in another way.

(6) The following are not to be provided to the Local Court—

(a) a document that formed part of the application for the dedicated encrypted criminal communication device prohibition order,

(b) the reasons recorded by the authorised magistrate for making the order.

(7) Subsection (6) does not prevent the Commissioner of Police from providing information to the Local Court if the Commissioner considers it to be relevant to the application.

(8) An application for the revocation of a dedicated encrypted criminal communication device prohibition order must not be made by the subject of the order within 6 months after—

(a) a copy of the order has been served on the subject of the order, or

(b) an application for the revocation of the order is refused by the Local Court.

20 Revocation of dedicated encrypted criminal communication device prohibition order on application of Commissioner of Police or oversight commissioner

(1) Either of the following persons may apply, at any time, to the Local Court to have a dedicated encrypted criminal communication device prohibition order revoked—

(a) the Commissioner of Police,

(b) the oversight commissioner.

(2) For an application made under subsection (1), the following persons are the respondent to the application—

(a) for an application made by the Commissioner of Police—the oversight commissioner,

(b) for an application made by the oversight commissioner—the Commissioner of Police.

(3) The Local Court may require the applicant to provide the Court with a copy of the dedicated encrypted criminal communication device prohibition order.

(4) The Local Court may—

(a) affirm the dedicated encrypted criminal communication device prohibition order, or

(b) vary the term of the order, or

(c) revoke the order.

(5) The Local Court may revoke the dedicated encrypted criminal communication device prohibition order only if satisfied—

(a) the order is unreasonably onerous in the circumstances, or

(b) the subject of the order is not likely to use a dedicated encrypted criminal communication device to avoid law enforcement detection of criminal activity, or

(c) the risk of the subject of the order using a dedicated encrypted criminal communication device to avoid law enforcement detection of criminal activity could be mitigated in another way.

(6) The following are not to be provided to the Local Court—

(a) a document that formed part of the application for the dedicated encrypted criminal communication device prohibition order,

(b) the reasons recorded by the authorised magistrate for making the order.

(7) Subsection (6) does not prevent the Commissioner of Police from providing information to the Local Court if the Commissioner considers it to be relevant to the application.

Part 6 Reports

21 Reports to authorised magistrate and oversight commissioner

(1) The Commissioner of Police must ensure a report about a dedicated encrypted criminal communication device prohibition order is given to—

(a) the authorised magistrate who issued the order, and

(b) the oversight commissioner.

(2) The report must include the following information about the order—

(a) the number of searches carried out under the order,

(b) details of each search, including the following—

(i) the date on which the search took place,

(ii) the location of the search,

(iii) the person, vehicle or premises searched,

(iv) the type and duration of the search,

(v) the number of persons, excluding police officers, who were present at the search or were adversely affected by the search,

(c) details of evidence uncovered by the searches and the use made or to be made of the evidence,

(d) details of anything seized,

(e) whether an application was made to revoke the order and the results of the application.

(3) The report must be provided as soon as practicable, but not more than 60 days, after the order ceases to be in force because it has expired or been revoked.

Part 7 Miscellaneous

22 Oversight commissioner

(1) The Secretary, in consultation with the Attorney General, must appoint an oversight commissioner.

(2) The oversight commissioner must be employed in the Public Service on a full-time or part-time basis.

(3) A person cannot be employed as the oversight commissioner unless the person is—

(a) an Australian legal practitioner with at least 7 years' legal practice experience, and

(b) either—

(i) a Judge or other judicial officer, or a former Judge or other judicial officer, of a superior court of record of the State or of another State or Territory or of Australia, or

(ii) qualified to be appointed as a Judge or other judicial officer of a court referred to in subparagraph (i).

(4) A person cannot be employed as the oversight commissioner if the person is a member of the NSW Police Force.

(5) The oversight commissioner has the functions conferred or imposed on the commissioner by or under this Act or another Act.

(6) The Secretary may appoint additional oversight commissioners under this section on a temporary basis to cover an absence of the oversight commissioner or in other circumstances as the Secretary sees fit.

23 Authorised magistrate

(1) A magistrate may, by written instrument, consent to be declared by the Attorney General under this section.

(2) The Attorney General may, by written instrument, declare magistrates in relation to whom consents are in force under this section to be authorised magistrates for the purposes of this Act.

(3) An authorised magistrate has, in relation to the exercise of a function conferred on an authorised magistrate by this Act, the same protection and immunity as a magistrate has in relation to proceedings in the Local Court.

(4) A magistrate who has given consent under this section may, by written instrument, revoke the consent.

(5) A declaration of an authorised magistrate under this section may not be revoked by the Attorney General.

(6) However, the declaration of a magistrate as an authorised magistrate is revoked if—

(a) the authorised magistrate ceases to be a magistrate, or

(b) the magistrate revokes the magistrate's consent to be an authorised magistrate, or

(c) the Chief Magistrate notifies the Attorney General that the magistrate should not continue to be an authorised magistrate.

(7) To avoid doubt—

(a) the selection of an authorised magistrate to exercise a particular function conferred on authorised magistrates is not to be made by the Attorney General or another Minister, and

(b) the exercise of that particular function is not subject to the control and direction of the Attorney General or another Minister.

24 Approved forms

The Secretary may approve forms for use under this Act.

25 Review of Act

(1) The Minister must conduct a review of this Act to determine whether—

(a) the policy objectives of the Act remain valid, and

(b) the terms of the Act remain appropriate for securing the objectives.

(2) The review must be commenced as soon as practicable after the period of 2 years after the commencement date.

(3) A report on the outcome of the review must be tabled in each House of Parliament within 12 months after the end of the period.

(4) In this section—

commencement date means the date on which this Act commences.

26 Regulations

The Governor may make regulations, not inconsistent with this Act, about—

(a) a matter that, by this Act, is required or permitted to be prescribed, or

(b) a matter that is necessary or convenient to be prescribed for carrying out or giving effect to this Act.

Schedule 1 Dictionary

application day means the day on which the application for the dedicated encrypted criminal communication device prohibition order was made.

authorised magistrate means a magistrate in relation to whom the following are in force—

(a) a consent under section 23(1),

(b) a declaration under section 23(2).

computer means an electronic device for storing, processing or transferring information.

dedicated encrypted criminal communication device has the same meaning as in the *Crimes Act 1900*, section 192O.

dedicated encrypted criminal communication device prohibition order means an order made under section 12.

eligible person means a person who—

(a) has been convicted of a serious criminal offence, and

(b) is at least 18 years of age on the application day.

exercise a function includes perform a duty.

foreign jurisdiction means a jurisdiction other than New South Wales.

function includes a power, authority or duty.

oversight commissioner means the oversight commissioner appointed under section 22.

Secretary means the Secretary of the Department of Communities and Justice.

senior police officer means a police officer who holds the rank of Superintendent or above, including the Commissioner of Police.

serious criminal offence means—

(a) a serious violence offence within the meaning of the *Crimes Act 1900*, section 93S(1), or

(b) an offence under the *Crimes Act 1900*, Part 3A, Division 5, or

(c) a money laundering offence under the *Crimes Act 1900*, Part 4AC, or

(d) a serious drug offence within the meaning of the *Drug Supply Prohibition Order Pilot Scheme Act 2020*, or

(e) an offence under the *Crimes Act 1900*, section 192P, or

(f) an offence under the *Firearms Act 1996*, section 51, 51B, 51BA or 51BB, or

(g) an offence under the *Weapons Prohibition Act 1998*, section 23A or 23B, or

(h) a serious Commonwealth offence within the meaning of the *Crimes Act 1914* of the Commonwealth, section 15GE, or

(i) an offence under a law of a foreign jurisdiction that is prescribed by the regulations to be a serious

criminal offence for this Act.

subject, of an order, means the person against whom a dedicated encrypted criminal communication device prohibition order is made.

vehicle includes a vessel or an aircraft.

Schedule 2 Amendment of Crimes Act 1900 No 40

Part 4ABA

Insert before Part 4AC—

Part 4ABA Offences involving dedicated encrypted criminal communication devices

192N Definitions

In this Part—

dedicated encrypted criminal communication device—see section 192O.

serious criminal activity means the following, whether or not a person has been charged with or convicted of an offence—

(a) committing an offence that—

(i) is punishable by imprisonment for 5 years or more, and

(ii) is a serious criminal offence within the meaning of the *Criminal Assets Recovery Act 1990*, or

(b) obtaining material benefits from conduct that constitutes an offence under paragraph (a).

192O Meaning of "dedicated encrypted criminal communication device"

(1) For this Part, a ***dedicated encrypted criminal communication device*** means a mobile electronic device that—

(a) is specifically designed or equipped for use to facilitate communication, between persons reasonably suspected of being involved in serious criminal activity, to defeat law enforcement detection, and

(b) uses hardware modifications or software deployed on the device that—

(i) modifies the device's factory operating system, whether temporarily or permanently to block or replace key features usually available on the device's operating system, including, for example, voice call, web

browsers or geolocation services, and

(ii) enables encryption of communication between users, and

(c) is configured in a way that specifically impedes law enforcement access to information on the device.

Example for paragraph (c)—

- a duress password or PIN that will wipe data on the device
- use of a mobile service that is not able to be traced to an individual
- appears to be mobile phone that does not have an International Mobile Station Equipment Identity number

(2) A dedicated encrypted criminal communication device includes a device prescribed by the regulations for the purposes of this section.

(3) A dedicated encrypted criminal communication device does not include—

(a) a device if—

(i) the device has been designed, modified or equipped with software or security features, and

(ii) a reasonable person would consider the software or security features have been applied for a primary purpose other than facilitating communication between persons involved in criminal activity to defeat law enforcement detection, or

(b) a device of a kind prescribed by the regulations as not being a dedicated encrypted criminal communication device.

192P Possession of dedicated encrypted criminal communication devices for certain purposes

(1) A person commits an offence if—

(a) the person possesses a dedicated encrypted criminal communication device, and

(b) there are reasonable grounds to suspect the possession of the dedicated encrypted criminal communication device was to commit or facilitate serious criminal activity.

Maximum penalty—Imprisonment for 3 years.

(2) Without limiting subsection (1)(b), matters that may be considered in determining whether there are reasonable grounds to suspect the possession of the dedicated encrypted criminal communication device to commit or facilitate a

serious criminal activity include the following—

(a) a service attached to the dedicated encrypted criminal communication device is in a false name,

(b) the dedicated encrypted criminal communication device was purchased or obtained from—

(i) a criminal network, or

(ii) a person who is reasonably suspected of supplying dedicated encrypted criminal communication devices to persons involved in criminal activity,

(c) a person is in possession of indications of drug supply,

(d) contemporaneous possession of prohibited firearms,

(e) contemporaneous possession of child abuse material.

(3) It is a defence to a prosecution for an offence under this section if the defendant satisfies the court that the defendant had possession of the dedicated encrypted criminal communication device—

(a) in the ordinary course of the defendant's duties as an officer, employee or agent of a government agency or public authority, or

(b) to supply to, or in partnership or agreement with, a government agency.

(4) To avoid doubt, for subsection (3)(a) and (b), a government agency includes—

(a) a government agency of this State, and

(b) a government agency of the Commonwealth or another State or a Territory.

192Q Proof of particular offence not required

To avoid doubt, it is not necessary for the purposes of the offence in section 192P(1) for the prosecution to prove that a particular offence was being committed or planned to be committed using the dedicated encrypted criminal communication device.

192R Review of Part

(1) The Minister must conduct a review of this Part to determine whether—

(a) the policy objectives of the relevant provisions remain valid, and

(b) the terms of the Part remain appropriate for securing the objectives.

(2) The review must be commenced as soon as practicable after the period of 2 years after the commencement date.

(3) A report on the outcome of the review must be tabled in each House of Parliament within 12 months after the end of the period.

(4) In this section—

commencement date means the date on which the *Dedicated Encrypted Criminal Communication Device Prohibition Orders Act 2022*, Schedule 2 commences.

Schedule 3 Amendment of Law Enforcement (Powers and Responsibilities) Act 2002 No 103

[1] Section 3 Interpretation

Insert in alphabetical order in section 3(1)—

DECCD access order, for Part 5A, see section 80A.

DECCD offence, for Part 5A, see section 80A.

relevant person, for Part 5A, see section 80A.

[2] Part 5A

Insert after Part 5—

Part 5A DECCD Access Orders

Division 1 Preliminary

80A Definitions

In this Part—

DECCD access order means an order issued under Division 4.

DECCD offence means an offence under the *Crimes Act 1900*, section 192P(1).

relevant person, for a DECCD access order, means a person specified in the order as being subject to a direction under the order.

Division 2 Applications for DECCD access orders

80B General matters for applications for DECCD access orders

A police officer may apply to a Magistrate for a DECCD access order if the police officer—

(a) has reasonable grounds to suspect the person specified in the order is—

(i) in possession of a device suspected of being a dedicated encrypted criminal communication device, and

(ii) committing a DECCD offence, and

(b) considers the making of the DECCD access order will assist law enforcement in determining whether the device is a dedicated encrypted criminal communication device.

80C Applications for DECCD access orders in person

(1) An application for a DECCD access order may be made in person.

(2) An application for a DECCD access order made under this section must be in writing in the form prescribed by the regulations.

(3) A Magistrate must not issue a DECCD access order under this section unless the information given by the applicant in or in connection with the application is verified before the Magistrate—

(a) on oath or affirmation, or

(b) by affidavit.

(4) A Magistrate may administer an oath or affirmation or take an affidavit for the purposes of an application for a DECCD access order.

80D Applications for DECCD access orders by email or other electronic means

(1) An application for a DECCD access order may be made—

(a) by email, or

(b) in another way prescribed by the regulations for this section.

(2) An application for a DECCD access order made under this section must be in the form prescribed by the regulations.

(3) A Magistrate must not issue a DECCD access order under this section unless the information given by the applicant in or in connection with the application is verified—

(a) before the Magistrate on oath or affirmation, or

(b) by affidavit.

(4) A Magistrate may administer an oath or affirmation or take an affidavit for the

purposes of an application for a DECCD access order.

(5) The requirement under subsection (3) for information to be verified before a Magistrate is taken to be satisfied if—

(a) the applicant appears before the Magistrate by audio visual link or telephone, and

(b) the Magistrate administers the oath or affirmation by the same means.

(6) If the Magistrate issues the order on an application made under this section, the Magistrate may—

(a) email the signed order to the applicant, or

(b) provide the signed order to the applicant in any way prescribed by the regulations.

80E Applications for DECCD access orders by telephone

(1) An application for a DECCD access order may be made by telephone if it is not practicable for the application to be made—

(a) in person under section 80C, or

(b) by email or in another way under section 80D.

Note—

Telephone includes radio, facsimile and any other communication device.

(2) A Magistrate must not issue a DECCD access order on an application made by telephone unless the Magistrate is satisfied—

(a) the DECCD access order is required urgently, and

(b) it is not practicable for the application to be made in person under section 80C or by email or in another way under section 80D.

(3) If it is not practicable for an application for a DECCD access order to be made by telephone directly to a Magistrate, the application may be transmitted to the Magistrate by another person on behalf of the applicant.

(4) A Magistrate who issues a DECCD access order on an application made by telephone must—

(a) complete and sign the DECCD access order, and

(b) either—

(i) give the DECCD access order to the person who made the application, or

(ii) inform the person of the terms of the DECCD access order and the date and time when it was signed

(5) If a DECCD access order is issued on an application made by telephone and the applicant was not given the DECCD access order, the applicant must—

(a) complete a form of DECCD access order in the terms indicated by the Magistrate under subsection (4), and

(b) write on the form—

(i) the name of the Magistrate, and

(ii) the date and time the DECCD access order was signed.

(6) A form of DECCD access order completed under subsection (5) is taken to be a DECCD access order issued in accordance with this Act.

(7) A DECCD access order must be given by a Magistrate by email, if the facilities to do so are readily available, and the emailed copy is taken to be the original document.

80F Information in applications for DECCD access orders

(1) An application for a DECCD access order must include the following information—

(a) the name of the applicant,

(b) details of the person in relation to whom it is proposed the DECCD access order will be issued,

(c) particulars of the grounds on which the application is based, including the grounds for suspecting a DECCD offence is being committed,

(d) other information required by the regulations.

(2) If the person in relation to whom it is proposed the DECCD access order will be issued is under the age of 18 years, the application must be accompanied by a document signed by a police officer of the rank of Inspector or above authorising the applicant to make the application.

(3) The applicant must provide, either orally or in writing, any further information the Magistrate requires about the grounds on which the DECCD access order is being sought.

(4) Nothing in this section requires an applicant for a DECCD access order to disclose the identity of a person from whom information was obtained if the applicant is satisfied the disclosure might jeopardise the safety of any person.

80G False or misleading information in applications

(1) A person must not, in or in connection with an application for a DECCD access order, give information to a Magistrate that the person knows to be false or misleading in a material particular.

Maximum penalty—100 penalty units or imprisonment for 2 years, or both.

(2) This section applies whether or not the information given is also verified on oath or affirmation or by affidavit.

80H Further application for DECCD access order after refusal

(1) If an application by a person for a DECCD access order is refused by a Magistrate, the person or another person who is aware of the application may not make a further application for the same DECCD access order unless the further application provides additional information that justifies the making of the further application.

(2) Only one further application may be made in a particular case.

Division 3 Determining applications for DECCD access orders

80I Matters to be considered in determining reasonable grounds for digital evidence orders

A Magistrate, when determining whether there are reasonable grounds to issue a DECCD access order, must consider the reliability of the information on which the application is based, including the nature of the source of the information.

80J Decisions about applications for DECCD access orders

(1) The Magistrate must—

(a) consider the application for the DECCD access order, and

(b) decide whether or not to grant the application and issue a DECCD access order.

(2) The Magistrate may grant an application for a DECCD access order only if the Magistrate is satisfied—

(a) there are reasonable grounds for suspecting the person specified in the application is—

(i) in possession of a device suspected of being a dedicated encrypted criminal communication device, and

(ii) committing a DECCD offence, and

(b) considers the making of the DECCD access order will assist law enforcement in determining whether the device is a dedicated encrypted criminal communication device.

(3) If the Magistrate grants the application, the Magistrate must issue a DECCD access order to the applicant.

Division 4 Issue of DECCD access orders

80K Form of DECCD access orders

(1) A DECCD access order must be in the form prescribed by the regulations.

(2) Without limiting subsection (1), a DECCD access order must specify any conditions imposed in relation to the execution of the DECCD access order.

80L Term of DECCD access order

A DECCD access order remains in force for a period of 7 business days after it is issued.

80M Effect of DECCD access order

(1) A DECCD access order authorises a police officer to—

(a) examine the device to which the order applies, and any data accessible from the device, to determine whether the device is a dedicated encrypted criminal communication device, and

(b) direct the relevant person for the order to give the officer any information or assistance that is reasonable and necessary to enable the officer to access data held in or accessible from a device specified in, or within the scope of, the order.

(2) Without limiting subsection (1)(b), the executing officer may require the relevant person to provide reasonable and necessary assistance in accessing data on a computer that is secured by biometric means, including, for example, fingerprints or retina scans.

(3) To avoid doubt—

(a) information provided by a relevant person under subsection (1) to access data held in or accessible from a device may be used only for that purpose and no other purpose, and

(b) this section is subject to any other provision of this Act or another Act that provides for how a police officer may take particulars that are necessary to

identify a person.

Note—

See, for example, Part 10, which provides for taking of identification particulars from persons in custody and other offenders, including section 136, which provides for identification particulars of children under 14 years.

80N Duty to show DECCD access order

A person executing a DECCD access order must produce the DECCD access order for inspection by the relevant person for the order if requested by the person.

80O Failure to comply with DECCD access order

(1) A relevant person for a DECCD access order must not, without reasonable excuse—

(a) fail to comply with a direction given by the executing officer for the order, in accordance with the order, or

(b) give the executing officer information that is false or misleading in a material particular in purported compliance with a direction given by the executing officer, unless the person informs the executing officer the information is false or misleading.

Maximum penalty—100 penalty units or imprisonment for 5 years, or both.

(2) Without limiting subsection (1), it is not a reasonable excuse for a relevant person for a DECCD access order to fail to comply with the order or a requirement made in accordance with the order on the ground that complying with the order or the requirement would tend to incriminate the person or otherwise expose the person to a penalty.

Division 5 Miscellaneous

80P Record of proceedings before Magistrate

(1) A Magistrate who issues a DECCD access order must ensure a record is made of all relevant particulars of the grounds the Magistrate has relied on to justify the issue of the DECCD access order.

(2) A Magistrate who refuses to issue a DECCD access order must ensure a record is made of all relevant particulars of the grounds the Magistrate has relied on to justify the refusal to issue the DECCD access order.

(3) A matter that might disclose the identity of a person must not be recorded under this section if the Magistrate is satisfied making the record might jeopardise the safety of any person.

Note—

Regulations under section 238(3) may provide that certain documents, that may disclose the identity of persons, are not available for inspection.

80Q Defects in DECCD access orders

A DECCD access order is not invalidated by a defect, other than a defect that affects the substance of the DECCD access order in a material particular.

80R Imposition of functions on Magistrate not a conferral of jurisdiction

To avoid doubt, the imposition of a function on a Magistrate under this Part is not a conferral of jurisdiction on the Local Court.

80S Review of Part

(1) The Minister must conduct a review of this Part to determine whether—

(a) the policy objectives of the relevant provisions remain valid, and

(b) the terms of the Part remain appropriate for securing the objectives.

(2) The review must be commenced as soon as practicable after the period of 2 years after the commencement date.

(3) A report on the outcome of the review must be tabled in each House of Parliament within 12 months after the end of the period.

(4) In this section—

commencement date means the date on which the *Dedicated Encrypted Criminal Communication Device Prohibition Orders Act 2022*, Schedule 2 commences.

[3] Section 238 Regulations

Insert after section 238(3)(b)—

(c) the keeping of records in connection with the issue and execution of DECCD access orders, and

(d) the inspection and certification of records kept in connection with the issue and execution of DECCD access orders.

Schedule 4 Consequential amendment of other legislation

4.1 Criminal Procedure Act 1986 No 209

[1] Schedule 1 Indictable offences triable summarily

Insert at the end of Table 2, Part 2A, with appropriate item numbering—

Possession of dedicated encrypted criminal communication devices

An offence under the *Crimes Act 1900*, section 192P.

[2] Schedule 1, Table 2, Part 6

Insert at the end of the Part, with appropriate item numbering—

Law Enforcement (Powers and Responsibilities) Act 2002

An offence under the *Law Enforcement (Powers and Responsibilities) Act 2002*, section 80O.

4.2 Law Enforcement (Powers and Responsibilities) Regulation 2016

[1] Clause 4 Form of application for warrant or notice to produce

Insert at the end of the clause—

(5) For the Act, sections 80C(2) and 80D(2), an application for a DECCD access order is to be in the form set out in Schedule 1, Form 34, Part 1.

[2] Clause 6 Form of warrant or notice to produce

Insert at the end of the clause—

(4) For the Act, sections 80K(1), a digital evidence access order is to be in the form set out in Schedule 1, Form 34, Part 2.

[3] Clause 13 Keeping and inspection of records

Insert before clause 13(2)(d)—

(c2) a DECCD access order,

[4] Schedule 1 Forms

Insert at the end of the Schedule—

Form 34 Application for a DECCD access order

Part 1 Application

On [*Date*], I, [*Name and rank*] of [*Place of work*], apply for a DECCD access order in relation to [*Specify name of specified person.*], the specified person.

I swear/solemnly, sincerely and truly declare and affirm* that—

1 I have reasonable grounds for suspecting the specified person is in possession of a device being a DECCD, and

2 I have reasonable grounds for suspecting the specified person is committing a DECCD offence, and

3 The making of the DECCD access order will assist law enforcement in determining whether the device is a DECCD, and

4 The specified person meets the criteria of section 80J of the *Law Enforcement (Powers and Responsibilities) Act 2002*.

I rely on the following grounds in support of this application: [*Insert the reasonable grounds on which the application for the DECCD access order is based. If space is insufficient, continue overleaf or attach a separate sheet.*]

[*5 and 6 are to be completed if a previous application for the order has been made and refused. Attach a copy of the previous application to this Form.*]

5 * The following are details of the refusal of a previous application—

6 * The additional information that I consider justifies the making of this further application is—

7 I seek that a certificate pursuant to clause 14 of the *Law Enforcement (Powers and Responsibilities) Regulation 2016* be issued, on the following grounds: [*Specify grounds*]

Sworn/declared and affirmed* before me on [*Date*] at [*Place*] in the State of New South Wales.

Applicant [*Print name and insert signature.*]

Justice of the Peace [*Print name and insert signature.*]

[*This application may be sworn before the magistrate to whom the application is made for the issue of the order. Any alterations, deletions or annexures should be initialled or signed by the applicant and witnessed by the justice of the peace.*]

[* *Delete if inapplicable.*]

Warning

It is an offence under section 76AG of the *Law Enforcement (Powers and Responsibilities) Act 2002* to give information in this application knowing it is false or misleading in a material particular. The maximum penalty is a fine of 100 penalty units or imprisonment for 2 years, or both.

Note—

In the case of an application by telephone (but not by facsimile), this Form of application should be completed by the magistrate for record purposes as if it were made in person by the applicant but not verified on oath or affirmation or by affidavit.

Part 2 Magistrate's record of application for a DECCD access order

On [*Date*] at [*Time*], I, the undersigned magistrate, received this application for a DECCD access order.

1 [*To be completed if the application was made by telephone.*]
The application was made by [*Specify how the application was made (eg facsimile, telephone).*] and I was/was not* satisfied that the order was required urgently and it was/was not* practicable for the application to be made in person.

2 [*To be completed if the magistrate required the applicant to provide further information concerning the grounds on which the order was sought.*]
*Further information provided by the applicant, as required by me, is attached.
*Particulars of further information orally provided by the applicant, as required by me, are as follows: [*Specify particulars.*]

3 On considering the application I found/did not find* that there were reasonable grounds for issuing the order.
[*If the order is issued—continue.*]

4 The relevant particulars of the grounds on which I relied to justify the issue of the order are as follows: [*Either identify or specify the relevant particulars of the grounds in the application that are relied on. If space is insufficient, continue overleaf or attach a separate sheet.*]

5 The order was issued at [*Time*] on [*Date*].

Authorised officer [*Print name and insert signature.*]

[* *Delete if inapplicable.*]

Note—

Return this Form, together with a copy of the order to the Local Court registry at which the order was issued or nearest to the place at which it was issued.