First print

New South Wales

Dedicated Encrypted Criminal Communication Device Prohibition Orders Bill 2022

Explanatory note

This explanatory note relates to this Bill as introduced into Parliament.

This Bill is cognate with the *Crimes Amendment (Money Laundering) Bill 2022*.

Overview of Bill

The object of this Bill is to prevent and disrupt organised and other serious crime by—

(a) giving police an investigative tool by establishing a scheme for dedicated encrypted criminal communication device prohibition orders that provide for investigations of criminal activity involving dedicated encrypted criminal communication devices, and

(b) making possession of a dedicated encrypted criminal communication device for the purpose of committing or facilitating serious criminal activity an offence, and

(c) setting out powers given by a dedicated encrypted criminal communication device prohibition order, and

(d) setting out the requirements and processes for an application for a dedicated encrypted criminal communication device prohibition order, and

(e) providing that a dedicated encrypted criminal communication device prohibition order may only be made by an authorised magistrate and the obligations on and requirements of the magistrate making the order, and

(f) providing for the revocation of a dedicated encrypted criminal communication device prohibition order, and

(g) providing for the reporting requirements of the Commissioner of Police about a dedicated encrypted criminal communication device prohibition order, and

(h) establishing the role of oversight commissioner and providing for the declaration of authorised magistrates.

Outline of provisions

Part 1 Preliminary

Clause 1 sets out the name, also called the short title, of the proposed Act.

Clause 2 provides for the commencement of the proposed Act.

Clause 3 provides for the Dictionary in the proposed Act, Schedule 1 to define certain words and expressions used in the proposed Act.

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

Clause 4 sets out the purpose of dedicated encrypted criminal communication device prohibition orders.

Clause 5 sets out the entry and search powers of a police officer in relation to a person against which a dedicated encrypted criminal communication device prohibition order is in force. A police officer may stop, detain and search the person, enter and search certain premises, stop, detain and search a vehicle in certain circumstances related to the person or premises and search a computer identified during a search. The *Law Enforcement (Powers and Responsibilities) Act 2002* applies to the search.

Clause 6 sets out powers of a police offer to give a direction to a person against whom a dedicated encrypted criminal communication device prohibition order is in force to assist the police officer to access and view data held in or accessible from a computer identified during the search or a computer seized under the order that the police officer has reasonable grounds to suspect is a dedicated encrypted criminal communication device. The clause makes it an offence to fail to comply with the direction with a maximum penalty of imprisonment for 3 years.

Clause 7 sets out powers of a police officer to seize and detain a thing under a dedicated encrypted criminal communication device prohibition order if the police officer is conducting a search under section 5 of the proposed Act.

Clause 8 sets out the circumstances in which a person against whom a dedicated encrypted criminal communication device prohibition order is in force must be given written notice about a search. The Commissioner of Police is responsible for ensuring the notice is given.

Part 3 Applications for dedicated encrypted criminal communication device prohibition orders

Clause 9 sets out the circumstances where a police officer may apply to particular magistrates for a dedicated encrypted criminal communication device prohibition order to be made against an eligible person. The police office must reasonably believe the eligible person is likely to use a dedicated encrypted criminal communication device to conceal criminal activity and the application must be approved by a senior police officer. The proposed section also sets out the circumstances in which an application must not be made against a person.

Clause 10 provides that an application for a dedicated encrypted criminal communication device prohibition order must be in the form of an affidavit. The proposed section sets out the matters that must be included in the form. The clause requires the application to be accompanied by a signed authorisation from a senior police officer.

Clause 11 sets out the notice requirements for an application for a dedicated encrypted criminal communication device prohibition order. The Commissioner of Police must give the person appointed under the proposed Act as the oversight commissioner a notice containing particular information. An authorised magistrate is required, after deciding an application, to forward the application, accompanying documents and affidavit to the oversight commissioner.

Part 4 Making of dedicated encrypted criminal communication device prohibition orders

Clause 12 provides for authorised magistrates to make dedicated encrypted criminal communication device prohibition orders. To make an order, the magistrate must be satisfied the subject of the order is an eligible person and likely to use a dedicated encrypted criminal communication device to conceal criminal activity. The magistrate must give the oversight commissioner reasonable opportunity to make a submission in relation to the making of an order. The magistrate may also seek advice from the oversight commissioner in relation to an order.

Clause 13 provides that an authorised magistrate may take any matter into account when deciding whether a person is likely to use a dedicated encrypted criminal communication device to avoid law enforcement detection of criminal activity.

Clause 14 provides for procedural matters relating to making dedicated encrypted criminal communication device prohibition orders. This includes that a decision of a dedicated encrypted criminal communication device prohibition order is not required to be decided in a courtroom and there is no requirement to inform the subject of the order about the application for the order.

Clause 15 sets out the requirements of an authorised magistrate to keep records of a dedicated encrypted criminal communication device prohibition order and provides for the rights of a person to have knowledge of an order or the particulars of an order.

Clause 16 sets out the mandatory particulars to be included in a dedicated encrypted criminal communication device prohibition order.

Clause 17 provides for the commencement and duration of a dedicated encrypted criminal communication device prohibition order and sets out the requirements to be met before power may be exercised under the order. The clause also sets out the record keeping requirements of the Commissioner of Police for the order.

Clause 18 provides for alternative ways of serving a dedicated encrypted criminal communication device prohibition order where reasonable steps to serve a copy of the order personally on the subject of the order have been unsuccessful.

Part 5 Revocation of dedicated encrypted criminal communication device prohibition orders

Clause 19 provides for an application for the revocation of a dedicated encrypted criminal communication device prohibition order by the subject of the order. The application may be made to the Local Court and the Commissioner of Police is the respondent to the application. The Local Court has the power to affirm, vary or revoke an order. The clause sets out the matters which the Local Court must be satisfied of for an order to be revoked and information that is not to be provided to the Court, subject to the discretion of the Commissioner of Police.

Clause 20 provides for the revocation of a dedicated encrypted criminal communication device prohibition order on application of the Commissioner of Police or person appointed under the proposed Act as the oversight commissioner. The Local Court has the power to affirm, vary or revoke an order. The clause sets out the matters which the Local Court must be satisfied of for an order to be revoked and information that is not to be provided to the Court, subject to the discretion of the Commissioner of Police.

Part 6 Reports

Clause 21 provides that the Commissioner of Police must ensure a report about a dedicated encrypted criminal communication device prohibition order is given to the authorised magistrate who issued the order and the oversight commissioner as soon as practicable within 60 days after the order ceases to be in force. The clause also provides for the particulars that must be included in the report, including details of the evidence uncovered by the searches and the use made or to be made of the evidence.

Part 7 Miscellaneous

Clause 22 provides for the appointment of an oversight commissioner by the Secretary in consultation with the Attorney General. The Secretary may appoint additional temporary oversight commissioners in circumstances the Secretary sees fit. The oversight commissioner must be employed in the Public Service, be an Australian legal practitioner with at least 7 years experience and be a judge or other judicial officer or former judge or other judicial officer or qualified to be appointed as a judge or other judicial officer of a superior court of record of Australia.The oversight commissioner must not be a member of the NSW Police Force. The functions of the oversight commissioner are conferred on them by the proposed Act or another Act.

Clause 23 provides for the declaration of a magistrate to be an authorised magistrate for the purposes of the proposed Act by the Attorney General with written consent from the magistrate. An authorised magistrate may revoke the consent by written instrument but the Attorney General may not revoke the declaration of an authorised magistrate. The clause provides for other ways a declaration may be revoked.

Clause 24 provides that the Secretary may approve forms under the proposed Act.

Clause 25 requires the Minister to review the proposed Act as soon as practicable after the period of 2 years after the commencement date of the proposed Act and a report on the outcome must be tabled in each House of Parliament within 12 months after the end of the period.

Clause 26 provides for the regulation-making powers under the proposed Act.

Schedule 1 Dictionary

Schedule 1 defines certain words and expressions used in the proposed Act.

Schedule 2 Amendment of Crimes Act 1900 No 40

Schedule 2 inserts proposed Part 4ABA to provide for offences involving dedicated encrypted criminal communication devices. The proposed part sets out the definitions of ***dedicated encrypted criminal communication device*** and ***serious criminal activity*** for offences or particular conduct involving a dedicated encrypted criminal communication device. Proposed section 192P makes it an offence to possess a dedicated encrypted criminal communication device in certain circumstances with a maximum penalty of imprisonment for 3 years. Proposed section 192Q provides that proof of a particular offence is not required for the prosecution to prove an offence under proposed section 192P(1). Proposed section 192R requires the Minister to review proposed Part 4ABA as soon as practicable after the period of 2 years after the commencement date of the proposed Act and a report on the outcome must be tabled in each House of Parliament within 12 months after the end of the period.

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

Schedule 3[2] inserts proposed Part 5A to provide for dedicated encrypted criminal communication access orders (***DECCD access orders***). Proposed Division 1 defines certain words and expressions for the proposed Part. Proposed Division 2 sets out the particulars for making an application for a DECCD access order and the information that must be included in the application. Proposed section 80G makes it an offence to provide false or misleading information to a Magistrate in connection with a DECCD access order with a maximum penalty of 100 penalty units or imprisonment for 2 years or both. Proposed Division 3 provides for the particulars a Magistrate must consider in determining a DECCD access order and requires the Magistrate to make a decision whether or not to grant the application for the order. Proposed Division 4 provides for the particulars for a DECCD access order that has been issued, including the form, duration and effect of the order. Proposed Section 80O makes it an offence to fail to comply with a DECCD access order with a maximum penalty of 100 penalty units or imprisonment for 5 years or both.

Proposed Division 5 provides for the record keeping requirements of a Magistrate in relation to an application for a DECCD access order and provides for the effect of a defect on the validity of a DECCD access order. Proposed section 80S requires the Minister to review proposed Part 5A as soon as practicable after the period of 2 years after the commencement date of the proposed Act and a report on the outcome must be tabled in each House of Parliament within 12 months after the end of the period. **Schedule 3[1]** makes a consequential amendment.

Schedule 3[3] inserts proposed section 238(3)(c) and (d) to provide that the keeping, inspection and certification of records in connection with a DECCD access order may be provided for by the Regulations.

Schedule 4 Consequential amendment of other legislation

Schedule 4.1 amends the *Criminal Procedure Act 1986* to allow for offences under the following to be dealt with summarily—

(a) the *Crimes Act 1900*, section 192P,

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

Schedule 4.2[1] and [2] insert proposed clauses 4(5) and 6(5) into the *Law Enforcement (Powers and Responsibilities) Regulation 2016* to provide that an application for a DECCD access order and a digital evidence access order must be in the prescribed form. **Schedule 4.2[4]** inserts the prescribed form into the *Law Enforcement (Powers and Responsibilities) Regulation 2016*, Schedule 1.

Schedule 4.2[3] inserts proposed clause 13(2)(c2) into the *Law Enforcement (Powers and Responsibilities) Regulation 2016* to provide for the keeping and inspection of records of dedicated encrypted criminal communication device access orders.