Passed by both Houses

New South Wales

Law Enforcement (Powers and Responsibilities) Amendment (Digital Evidence Access Orders) Bill 2022

Contents

I certify that this public bill, which originated in the Legislative Assembly, has finally passed the Legislative Council and the Legislative Assembly of New South Wales.

Clerk of the Legislative Assembly.
Legislative Assembly,
Sydney, *, 2022*

New South Wales

Law Enforcement (Powers and Responsibilities) Amendment (Digital Evidence Access Orders) Bill 2022

Act No , 2022

An Act to amend the *Law Enforcement (Powers and Responsibilities) Act 2002* to provide for digital evidence access orders; and for related purposes.

I have examined this bill and find it to correspond in all respects with the bill as finally passed by both Houses.

Assistant Speaker of the Legislative Assembly.

The Legislature of New South Wales enacts—

1 Name of Act

This Act is the *Law Enforcement (Powers and Responsibilities) Amendment (Digital Evidence Access Orders) Act 2022*.

2 Commencement

This Act commences on 1 February 2023.

Schedule 1 Amendment of Law Enforcement (Powers and Responsibilities) Act 2002 No 103

[1] Section 3 Interpretation

Insert in alphabetical order in section 3(1)—

computer, for Part 5, Division 4A—see section 76AA.

digital evidence access order, for Part 5—see section 46.

eligible applicant, for Part 5—see section 46.

eligible issuing officer, for Part 5—see section 46.

executing officer, for Part 5—see section 46.

search warrant, for Part 5, Division 4A—see section 76AA.

specified person, for Part 5, Division 4A—see section 76AA.

[2] Section 46 Interpretation

Omit the definitions of ***eligible applicant***, ***eligible issuing officer*** and ***executing officer***.

Insert instead in alphabetical order—

digital evidence access order means an order issued under Division 4A.

eligible applicant means—

(a) for a covert search warrant or a digital evidence access order in connection with the covert search warrant—a person authorised under section 46C to apply for the covert search warrant, or

(b) for a criminal organisation search warrant or a digital evidence access order in connection with the criminal organisation search warrant—a police officer authorised under section 46D to apply for the criminal organisation search warrant, or

(c) for a search warrant issued under Part 11, Division 1 for suspected drug premises or a digital evidence access order in connection with the search warrant—a police officer authorised under section 140 to apply for the search warrant, or

(d) for a digital evidence access order in connection with a search warrant under the *Crime Commission Act 2012*, section 17(2)—an executive officer under that Act, or

(e) for any other search warrant or a digital evidence access order in connection with the search warrant—any police officer.

eligible issuing officer means—

(a) for a covert search warrant or a digital evidence access order in connection with the covert search warrant—an eligible Judge, or

(b) for a criminal organisation search warrant or a digital evidence access order in connection with the criminal organisation search warrant—an eligible Judge, or

(c) for a search warrant under the *Crime Commission Act 2012*, section 17(2) or a digital evidence access order in connection with the search warrant—an authorised officer, or

(d) for any other search warrant or a digital evidence access order in connection with the search warrant—an authorised officer, or

(e) for a notice to produce issued under Division 3—an authorised officer.

executing officer means—

(a) for a covert search warrant or a digital evidence access order in connection with a covert search warrant—

(i) any police officer, or

(ii) any member of staff of the Law Enforcement Conduct Commission if the applicant for the warrant was authorised under section 46C(1)(b) to make the application, or

(iii) a member of staff of the New South Wales Crime Commission if the applicant for the warrant was authorised under section 46C(1)(c) to make the application, or

(b) for a search warrant under the *Crime Commission Act 2012*, section 17(2) or a digital evidence access order in connection with the search warrant—an officer of the Commission under that Act, or

(c) for any other warrant or a digital evidence access order in connection with the warrant—any police officer.

[3] Section 74 Report to eligible issuing officer on execution of warrant other than covert search warrant

Insert after section 74(1)(d)—

(d1) if a digital evidence access order was issued in connection with the warrant—setting out a brief description of the use of the order, and

[4] Section 74A Report to eligible issuing officer on execution of covert search warrant

Insert after section 74A(1)(c)—

(c1) if a digital evidence access order was issued in connection with the warrant—setting out a brief description of the use of the order, and

[5] Part 5, Division 4A

Insert after Division 4—

Division 4A Digital evidence access orders

Subdivision 1 Preliminary

76AA Definitions

In this Division—

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

search warrant means—

(a) a search warrant issued under this Act, or

(b) a search warrant issued under any of the following provisions—

(i) the *Confiscation of Proceeds of Crime Act 1989*, section 36 or 67,

(ii) the *Crime Commission Act 2012*, section 17,

(iii) the *Criminal Assets Recovery Act 1990*, section 38 or 45,

(iv) the *Prevention of Cruelty to Animals Act 1979*, section 24F,

(v) the *Restricted Premises Act 1943*, section 13,

(vi) the *Security Industry Act 1997*, Part 3B,

(vii) the *Tattoo Parlours Act 2012*, section 30B.

(viii) the *Unlawful Gambling Act 1998*, section 40,

specified person, for a digital evidence access order, means a person, or a class of persons, specified in the order as being subject to a direction under the order.

Subdivision 2 Applications for digital evidence access orders

76AB General matters for applications for digital evidence access orders

(1) An eligible applicant may apply for a digital evidence access order, in connection with the following warrants, for authority for an executing officer to issue a direction mentioned in section 76AM(1) in relation to a computer that may be found, or has been found, in the execution of the warrant—

(a) a search warrant,

(b) a crime scene warrant.

(2) An application for a digital evidence access order is made in connection with a search warrant or crime scene warrant if the application is made—

(a) in relation to a searchable offence—

(i) at the same time as the application for the search warrant for a searchable offence, or

(ii) after the search warrant for the searchable offence has been issued, whether before or after the warrant is executed, or

(b) in relation to an offence mentioned in section 94(1)(a) or (b)—

(i) at the same time as the application for the crime scene warrant for the offence, or

(ii) after the crime scene warrant for the offence has been issued, whether before or after the warrant is executed, or

(c) in relation to a matter being investigated under the *Crime Commission Act 2012*—at the same time as the application for the search warrant or after the search warrant has been issued, whether before or after the warrant is executed.

76AC Applications for digital evidence access orders in person

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

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

(3) An eligible issuing officer must not issue a digital evidence access order under this section unless the information given by the applicant in or in connection with the application is verified before the eligible issuing officer—

(a) on oath or affirmation, or

(b) by affidavit.

(4) An eligible issuing officer may administer an oath or affirmation or take an affidavit for the purposes of an application for a digital evidence access order.

76AD Applications for digital evidence access orders by email or other electronic means

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

(3) An eligible issuing officer must not issue a digital evidence access order under this section unless the information given by the applicant in or in connection with the application is verified—

(a) before the eligible issuing officer on oath or affirmation, or

(b) by affidavit.

(4) An eligible issuing officer may administer an oath or affirmation or take an affidavit for the purposes of an application for a digital evidence access order.

(5) The requirement under subsection (2) for information to be verified before an eligible issuing officer is taken to be satisfied if—

(a) the applicant appears before the eligible issuing officer by audio visual link or telephone, and

(b) the eligible issuing officer administers the oath or affirmation by the same means.

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

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

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

76AE Applications for digital evidence access orders by telephone

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

(a) in person under section 76AC, or

(b) by email or in another way under section 76AD.

Note— ***Telephone*** includes radio, facsimile and any other communication device.

(2) An eligible issuing officer must not issue a digital evidence access order on an application made by telephone unless the eligible issuing officer is satisfied—

(a) the digital evidence access order is required urgently, and

(b) it is not practicable for the application to be made in person under section 76AC or by email or in another way under section 76AD.

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

(4) An eligible issuing officer who issues a digital evidence access order on an application made by telephone must—

(a) complete and sign the digital evidence access order, and

(b) either—

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

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

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

(a) complete a form of digital evidence access order in the terms indicated by the eligible issuing officer under subsection (5), and

(b) write on it—

(i) the name of the eligible issuing officer, and

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

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

(7) A digital evidence access order must be given by an eligible issuing officer by email, if the facilities to do so are readily available, and the emailed copy is taken to be the original document.

76AF Information in applications for digital evidence access orders

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

(a) the name of the applicant,

(b) details of the search warrant or crime scene warrant to which the application is connected,

(c) details of the specified person in relation to whom it is proposed the digital evidence access order will be issued,

(d) particulars of the grounds on which the application is based, including the grounds for suspecting—

(i) for a digital evidence access order in connection with a search warrant under the *Crime Commission Act 2012*—material connected with a matter being investigated under that Act is held in or accessible from the computer to which the application relates, or

(ii) otherwise—evidential material is held in or accessible from the computer to which the application relates,

(e) if a previous application for the same digital evidence access order was refused—details of the refusal and any additional information required by section 76AH,

(f) other information required by the regulations.

(2) If the specified person to whom it is proposed the digital evidence 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 eligible issuing officer requires about the grounds on which the digital evidence access order is being sought.

(4) Nothing in this section requires an applicant for a digital evidence 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.

76AG False or misleading information in applications

(1) A person must not, in or in connection with an application for a digital evidence access order, give information to an eligible issuing officer 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.

76AH Further application for digital evidence access order after refusal

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

(2) However, a further application may be made to a Magistrate following a refusal to issue a digital evidence access order by an eligible issuing officer who is not a Magistrate, whether or not additional information is provided in the further application.

(3) Subsection (2) does not apply to a digital evidence access order in connection with—

(a) a covert search warrant, or

(b) a criminal organisation search warrant.

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

Subdivision 3 Determining applications for digital evidence access orders

76AI Matters to be considered in determining reasonable grounds for digital evidence orders

An eligible issuing officer, when determining whether there are reasonable grounds to issue a digital evidence access order, must consider the reliability of the information on which the application is based, including the nature of the source of the information.

76AJ Decisions about applications for digital evidence access orders

(1) The eligible issuing officer must—

(a) consider the application for the digital evidence access order, and

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

(2) The eligible issuing officer may grant an application for a digital evidence access order only if—

(a) the order will authorise an executing officer to issue a direction mentioned in section 76AM(1) in relation to a computer that has been found, or may be found, in the execution of a search warrant or crime scene search warrant that has already been issued or will be issued at the same time as the order, and

(b) the eligible issuing officer is satisfied there are reasonable grounds for suspecting evidential material is held in, or is accessible from, the computer, and

(c) the eligible issuing officer is satisfied the specified person in relation to whom it is proposed the digital evidence access order will be issued is—

(i) reasonably suspected of having committed the offence stated in the search warrant or crime scene search warrant, 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

(d) the eligible issuing officer is satisfied the specified person in relation to whom it is proposed the digital evidence access order will be issued 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, or accessible from, the computer.

(3) If the eligible issuing officer grants the application, the officer must issue a digital evidence access order to the applicant.

Subdivision 4 Issue of digital evidence access orders

76AK Form of digital evidence access orders

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

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

76AL Term of digital evidence access order

(1) A digital evidence access order remains in force for a period of—

(a) for an order issued in connection with a covert search warrant—10 days after it is issued, or

(b) for any other order—7 business days after it is issued.

(2) A digital evidence access order may be extended by an authorised officer, on application by the executing officer, for no more than 3 additional periods of 7 business days.

(3) An application for a further digital evidence access order may be made in relation to the same computer.

76AM Effect of digital evidence access order

(1) The executing officer for a digital evidence access order may direct the specified person to—

(a) give the officer any information or assistance reasonable and necessary to enable the officer to access data held in or accessible from a computer specified in, or within the scope of, the order, or

(b) give the officer any information or assistance reasonable and necessary to allow the officer to—

(i) copy data from a computer specified in, or within the scope of, the order to another computer, or

(ii) convert the data into a documentary form or another form intelligible to a computer used by the officer.

(2) Without limiting subsection (1), the executing officer may require the specified 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 specified person under subsection (1) to access data held in or accessible from a computer 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 the age of 14 years.

76AN Duty to show digital evidence access order

(1) A person executing a digital evidence access order must produce the digital evidence access order for inspection by the specified person for the order if requested by the person.

(2) Subsection (1) does not apply to a digital evidence access order issued in connection with a covert search warrant.

76AO Failure to comply with digital evidence access order

(1) A specified person for a digital evidence access order must not, without reasonable excuse—

(a) fail to comply with a direction given, in accordance with the order, by the executing officer for 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 specified person for a digital evidence 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.

Subdivision 5 Miscellaneous

76AP Record of proceedings before eligible issuing officer

(1) An eligible issuing officer who issues a digital evidence access order must ensure a record is made of all relevant particulars of the grounds the eligible issuing officer has relied on to justify the issue of the digital evidence access order.

(2) An eligible issuing officer who refuses to issue a digital evidence access order must ensure a record is made of all relevant particulars of the grounds the eligible issuing officer has relied on to justify the refusal to issue the digital evidence access order.

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

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

76AQ Defects in digital evidence access orders

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

[6] Section 94A Application by occupier for review by a Magistrate of crime scene warrant

Insert "or a digital evidence access order in connection with the warrant" after "the warrant" in section 94A(3).

[7] Section 237A

Insert after section 237—

237A Review of certain provisions relating to digital evidence access orders

(1) The Minister must conduct a review of the relevant provisions to determine whether—

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

(b) the terms of the relevant provisions 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 *Law Enforcement (Powers and Responsibilities) Amendment (Digital Evidence Access Orders) Act 2022* commences.

relevant provisions means the provisions inserted by the *Law Enforcement (Powers and Responsibilities) Amendment (Digital Evidence Access Orders) Act 2022*.

[8] Section 238 Regulations

Insert after section 238(2)—

(3) Without limiting subsection (1), the regulations may provide for matters about digital evidence access orders, including—

(a) the keeping of records in connection with the issue and execution of digital evidence access orders, and

(b) the inspection and certification of records kept in connection with the issue and execution of digital evidence access orders.

Schedule 2 Amendment of Law Enforcement (Powers and Responsibilities) Regulation 2016

[1] Clause 4, heading

Omit "**or notice to produce**". Insert instead "**, notice to produce or order**".

[2] Clause 4(4)

Insert after clause 4(3)—

(4) For the Act, sections 76AC(2) and 76AD(2), an application for a digital evidence access order is to be in the form set out in Schedule 1, Form 33, Part 1.

[3] Clause 6, heading

Omit "**or notice to produce**". Insert instead "**, notice to produce or order**".

[4] Clause 6(3)

Insert after clause 6(2)—

(3) For the Act, sections 76AK(1), a digital evidence access order is to be in the form set out in Schedule 1, Form 33, Part 2.

[5] Clause 13 Keeping and inspection of records

Insert "or order" after "each warrant" in clause 13(1).

[6] Clause 13(1)(a) and (b)

Insert "or order" after "warrant" wherever occurring.

[7] Clause 13(1)(e)

Insert "or order" after "clause 9 or 10)".

[8] Clause 13(2)

Insert after clause 13(2)(c)—

(c1) a digital evidence access order,

[9] Schedule 1 Forms

Insert at the end of the Schedule—

Form 33 Application for a digital evidence access order

Part 1 Application

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

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

1 This digital evidence access order is made in connection with [*Specify warrant type and details.*]

2 The [*Specify warrant type and details*] [*has been issued OR will be issued at the same time as the order*]

3 I have reasonable grounds for suspecting evidential material is held in, or is accessible from, [*Specify the computer*], and that

4 The specified person meets the criteria of section 76AJ 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 digital evidence 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* [*Need not be completed if the previous application was made to an authorised officer who was not a Magistrate and this application is made to a Magistrate.*]

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

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 authorised officer 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 2 years imprisonment, or both.

Note— In the case of an application by telephone (but not by facsimile), this Form of application should be completed by the authorised officer 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 Authorised officer's record of application for a digital evidence access order

On [*Date*] at [*Time*], I, the undersigned authorised officer, received this application for a digital evidence 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 authorised officer 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.*]

6 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.

Schedule 3 Consequential amendment of Criminal Procedure Act 1986 No 209

Schedule 1 Indictable offences triable summarily

Insert at the end of Table 2, Part 6, with appropriate item numbering—

Law Enforcement (Powers and Responsibilities) Act 2002

An offence under the *Law Enforcement (Powers and Responsibilities) Act 2002*, section 76AG(1).