First print

New South Wales

Crimes and Other Legislation Amendment (Further Organised Crimes Reforms) Bill 2026

Explanatory note

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

Overview of Bill

The objects of this Bill are as follows—

(a) to amend the *Crime Commission Act 2012* (***the Act***) to—

  (i) increase penalties for certain offences, and

  (ii) clarify matters relating to contempt of the New South Wales Crime Commission (the ***Commission***),

(b) to amend the *Law Enforcement (Powers and Responsibilities) Act 2002* to provide for digital evidence access orders (organised crime),

(c) to amend the *Road Transport Act 2013* to support and facilitate the Intergovernmental Agreement on Identity Matching Services,

(d) to amend the *Roads Act 1993* to provide for the collection, use and disclosure of toll camera images.

Outline of provisions

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.

Schedule 1 Amendment of Crime Commission Act 2012 No 66

Schedule 1[1] increases the maximum penalty for the offence of failing to attend and answer questions at a hearing before the Commission when summoned as a witness to 40 penalty units or imprisonment for 4 years, or both.

Schedule 1[2] increases the maximum penalty for the offence of giving false or misleading evidence at a hearing before the Commission to 1,000 penalty units or imprisonment for 10 years, or both.

Schedule 1[3] increases the maximum penalty for offences under the Act, section 28(4), which concern compliance with a production notice served on certain persons in a government agency, to 40 penalty units or imprisonment for 12 months, or both.

Schedule 1[4] increases the maximum penalty for the offence of failing to comply with a production notice under the Act, section 29(9) to 40 penalty units or imprisonment for 12 months, or both.

Schedule 1[5] increases the maximum penalty for the offence of failing to comply with a condition imposed on the release of a witness by the Commissioner of the Commission (the ***Commissioner***) under the Act, section 37(3) to 40 penalty units or imprisonment for 4 years, or both.

Schedule 1[6] and [7] amend the Act, section 45 to—

(a) increase the maximum penalty for the offence of making a publication or disclosure of evidence in contravention of a direction given by the Commission to 200 penalty units or imprisonment for 4 years, or both, and

(b) clarify that the Local Court may prescribe the maximum fine regardless of the *Criminal Procedure Act 1986*, section 268.

Schedule 1[8] and [9] amend the Act, section 45A to—

(a) increase the maximum penalty for the offence of making a disclosure that contravenes an order made by the Commission restricting the disclosure of evidence or a record of evidence allowed to be disclosed under the Act, section 45A(3) or (4) to 200 penalty units or imprisonment for 4 years, or both, and

(b) clarify that the Local Court may prescribe the maximum fine regardless of the *Criminal Procedure Act 1986*, section 268.

Schedule 1[10] and [11] amend the Act, section 47C to provide that—

(a) in the exercise of the Commissioner's powers in relation to alleged contempt, a summons need not be issued against a person alleged to have committed contempt under the Act, section 47A (a ***contemnor***), and

(b) a contemnor does not need to be delivered into the custody of the governor of a correctional centre specified in a warrant issued by the Commissioner and instead may be detained in a correctional facility or elsewhere until the contemnor is brought before the Supreme Court.

Schedule 1[12] increases the maximum penalty for a contemnor failing to comply with a condition to which the release of the contemnor is subject to 40 penalty units or imprisonment for 4 years, or both.

Schedule 1[13] and [14] amend the Act, section 47G to—

(a) increase the maximum penalty for the offence of obstructing or disrupting the Commission to 200 penalty units or imprisonment for 4 years, or both, and

(b) clarify that the Local Court may prescribe the maximum fine regardless of the *Criminal Procedure Act 1986*, section 268.

Schedule 1[15] increases the maximum penalty to 100 penalty units or imprisonment for 2 years, or both, for the following offences—

(a) disclosing information about a production notice under the Act, section 28 or 29 that is likely to prejudice the investigation to which the notice relates,

(b) disclosing information about a summons under the Act, section 24 that is likely to prejudice the investigation to which the summons relates.

Schedule 1[16] provides that the Act, section 85(1) does not affect the capacity of a prosecutor to elect, under the *Criminal Procedure Act 1986*, for a prosecution for certain offences to be dealt with on indictment.

Schedule 2 Amendment of Law Enforcement (Powers and Responsibilities) Act 2002 No 103

Schedule 2[9] inserts proposed Division 4B, which provides for digital evidence access orders (organised crime) (***orders***), into Part 5.

Proposed Subdivision 1 inserts definitions of certain words and expressions used in the proposed division.

Proposed Subdivision 2 contains provisions relating to applications for orders. The proposed subdivision—

(a) provides for general matters for applications, and

(b) sets out how applications may be made in person, by email or other electronic means or by telephone, and

(c) sets out the required particulars of an application, and

(d) makes it an offence to give false or misleading information in an application or in connection with an application, with a maximum penalty of 100 penalty units or imprisonment for 2 years, or both, and

(e) provides that, if an application has been refused, a further application for the same order must not be made by the police officer who made the application or another police officer who is aware of the application other than in certain circumstances.

Proposed Subdivision 3 provides for how applications for orders may be determined, including matters that must be considered by an eligible issuing officer when deciding whether or not to grant the application.

Proposed Subdivision 4 contains provisions concerning the issuing of orders. The proposed subdivision—

(a) enables the regulations to prescribe the required form of an order, and

(b) provides for the term for which an order remains in force and sets out how an order may be extended, and

(c) sets out the effect of an order, and

(d) imposes a duty on the person executing an order to produce the order for inspection in certain circumstances, and

(e) makes it an offence to fail to comply, or to give false or misleading information in purported compliance, with a direction given in accordance with an order, with a maximum penalty of 100 penalty units or imprisonment for 7 years, or both.

Proposed Subdivision 5 provides for miscellaneous matters, including record-keeping requirements.

Schedule 2[1]–[7] and [10] make amendments consequential to Schedule 2[9].

Schedule 2[8] increases the maximum term of imprisonment to 7 years for the following offences—

(a) failing to comply with a digital evidence access order (warrant),

(b) giving false or misleading information in purported compliance with a digital evidence access order (warrant).

Schedule 3 Amendment of Criminal Procedure Act 1986 No 209

Schedule 3[1] makes an amendment consequential to Schedule 2[9].

Schedule 3[2] makes an amendment consequential to Schedule 1[1], [5], [6], [8], [12] and [13].

Schedule 4 Amendment of Road Transport Act 2013 No 18

Schedule 4[1]—

(a) omits provisions relating to the National Facial Biometric Matching Capability, and

(b) provides for the participation of authorised government agencies in face matching services, and

(c) permits the regulations to provide for further matters to facilitate participation in face matching services, and

(d) defines certain terms used in proposed section 271A.

Schedule 5 Amendment of Roads Act 1993 No 33

Schedule 5[2] inserts proposed Part 15B, which provides for the collection, storage and disclosure of toll camera images. The proposed part—

(a) defines certain terms used in the proposed part, including ***relevant information***, and

(b) sets out what photographs an approved toll camera is permitted to take, and

(c) makes it an offence for a person who acquires relevant information to a make record of, make use of or disclose the information other than in certain circumstances, with a maximum penalty of 50 penalty units, and

(d) sets out when a person is permitted to collect, store and disclose relevant information, and

(e) permits a person to disclose relevant information to an authorised agency in certain circumstances.

Schedule 5[1] makes an amendment consequential to Schedule 5[2].

First print

New South Wales

Crimes and Other Legislation Amendment (Further Organised Crimes Reforms) Bill 2026

Contents

This PUBLIC BILL, originated in the LEGISLATIVE ASSEMBLY and, having this day passed, is now ready for presentation to the LEGISLATIVE COUNCIL for its concurrence.

Clerk of the Legislative Assembly

Legislative Assembly

New South Wales

Crimes and Other Legislation Amendment (Further Organised Crimes Reforms) Bill 2026

No , 2026

A Bill for

An Act to amend the *Crime Commission Act 2012* to increase penalties for offences under that Act and clarify matters relating to contempt of the New South Wales Crime Commission; to amend the *Law Enforcement (Powers and Responsibilities) Act 2002* to provide for digital evidence access orders (organised crime); to amend the *Road Transport Act 2013* to support the Intergovernmental Agreement on Identity Matching Services; to amend the *Roads Act 1993* to provide for the collection, use and disclosure of toll camera images; and for related purposes.

The LEGISLATIVE COUNCIL has this day agreed to this Bill with/without amendment.

Clerk of the Parliaments

Legislative Council

The Legislature of New South Wales enacts—

1 Name of Act

This Act is the *Crimes and Other Legislation Amendment (Further Organised Crimes Reforms) Act 2026*.

2 Commencement

This Act commences as follows—

(a) for Schedules 2 and 3[1]—on a day or days to be appointed by proclamation,

(b) otherwise—on the date of assent to this Act.

Schedule 1 Amendment of Crime Commission Act 2012 No 66

[1] Section 25 Failure of witnesses to attend and answer questions etc

Omit the penalty.

Insert instead—

Maximum penalty—40 penalty units or imprisonment for 4 years, or both.

[2] Section 27 False or misleading evidence

Omit "not exceeding 500 penalty units or by imprisonment for a period not exceeding 5 years" from section 27(2).

Insert instead "of not more than 1,000 penalty units or imprisonment for not more than 10 years".

[3] Section 28 Commission may require information from certain government agencies

Omit section 28(4), penalty.

Insert instead—

Maximum penalty—40 penalty units or imprisonment for 12 months, or both.

[4] Section 29 Power to obtain documents and things

Omit section 29(9), penalty.

Insert instead—

Maximum penalty for subsection (9)—40 penalty units or imprisonment for 12 months, or both.

[5] Section 37 Conditional release of witness

Omit section 37(3), penalty.

Insert instead—

Maximum penalty for subsection (3)—40 penalty units or imprisonment for 4 years, or both.

[6] Section 45 Publication or disclosure of evidence

Omit section 45(3), penalty.

Insert instead—

Maximum penalty—200 penalty units or imprisonment for 4 years, or both.

[7] Section 45(3A)

Insert after section 45(3)—

(3A) The maximum fine specified in subsection (3) for an offence dealt with summarily applies regardless of the *Criminal Procedure Act 1986*, section 268.

[8] Section 45A Disclosure of evidence of accused about offence for which charged

Omit section 45A(6), penalty.

Insert instead—

Maximum penalty—200 penalty units or imprisonment for 4 years, or both.

[9] Section 45A(6A)

Insert after section 45A(6)—

(6A) The maximum fine specified in subsection (6) for an offence dealt with summarily applies regardless of the *Criminal Procedure Act 1986*, section 268.

[10] Section 47C Powers of Commissioner in relation to alleged contempt

Omit section 47C(5).

Insert instead—

(5) If the alleged contempt of the Commission is committed in the face or hearing of the Commissioner, a summons need not be issued against the contemnor but the Commissioner may direct that the contemnor—

(a) be immediately taken into custody in a correctional centre or elsewhere by—

(i) a member of the NSW Police Force, or

(ii) an officer of the Commission authorised by the Commissioner, and

Note— A person in custody may be given into the keeping of a correctional officer. See the *Crimes (Administration of Sentences) Act 1999*, section 250.

(b) be called on to show cause why the contemnor should not be dealt with under section 47B for the alleged contempt.

[11] Section 47C(7)(b)

Omit section 47C(7)(b) and (c).

Insert instead—

(b) for the contemnor to be detained in a correctional facility or elsewhere until the contemnor is brought before the Supreme Court.

[12] Section 47D Conditional release of contemnor

Omit section 47D(5), penalty.

Insert instead—

Maximum penalty—40 penalty units or imprisonment for 4 years, or both.

[13] Section 47G Obstruction or disruption of Commission

Omit the penalty.

Insert instead—

Maximum penalty—200 penalty units or imprisonment for 4 years, or both.

[14] Section 47G(2)

Insert at the end of section 47G—

(2) The maximum fine specified in subsection (1) for an offence dealt with summarily applies regardless of the *Criminal Procedure Act 1986*, section 268.

[15] Section 81 Disclosures prejudicing investigations

Omit section 81(1), penalty.

Insert instead—

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

[16] Section 85 Proceedings for offences

Insert after section 85(1)—

(1A) Subsection (1) does not affect the capacity of a prosecutor to elect, under the *Criminal Procedure Act 1986*, for a prosecution for an offence under section 25, 37(3), 45(3), 45A(6), 47D(5) or 47G(1) to be dealt with on indictment.

Schedule 2 Amendment of Law Enforcement (Powers and Responsibilities) Act 2002 No 103

[1] Whole Act, except as otherwise amended by this schedule

Omit "digital evidence access order" wherever occurring.

Insert instead "digital evidence access order (warrant)".

[2] Whole Act, except as otherwise amended by this schedule

Omit "digital evidence access orders" wherever occurring.

Insert instead "digital evidence access orders (warrant)".

[3] Section 3 Interpretation

Omit section 3(1), definitions of ***computer***, ***digital evidence access order*** and ***specified person***.

Insert in alphabetical order—

computer—

(a) for Part 5, Division 4A—see section 76AA, or

(b) for Part 5, Division 4B—see section 76AR.

digital evidence access order (organised crime), for Part 5, Division 4B—see section 76AR.

digital evidence access order (warrant), for Part 5, Division 4A—see section 46.

organised crime offence, for Part 5, Division 4B—see section 76AS.

serious offence, for Part 5, Division 4B—see section 76AR.

specified person—

(a) for Part 5, Division 4A—see section 76AA, or

(b) for Part 5, Division 4B—see section 76AR.

[4] Section 3(1), definitions of "eligible applicant" and "eligible Judge", paragraph (a)

Omit "Part 5" wherever occurring.

Insert instead "Part 5, Division 4A".

[5] Section 46 Interpretation

Insert after section 46(1), definition of ***eligible issuing officer***, paragraph (b)—

(b1) for a digital evidence access order (organised crime)—a Judge of the Local Court, or

[6] Section 46(1), definition of "executing officer", paragraph (d)

Omit "officer." from paragraph (c).

Insert instead—

officer, or

(d) for a digital evidence access order (organised crime)—any police officer.

[7] Part 5, Division 4A, heading

Insert "**(warrant)**" after "**orders**".

[8] Section 76AO Failure to comply with digital evidence access order

Omit "5 years" from section 76AO(1), penalty.

Insert instead "7 years".

[9] Part 5, Division 4B

Insert after section 76AQ—

Division 4B Digital evidence access orders (organised crime)

Subdivision 1 Preliminary

76AR Definitions

In this division—

computer has the same meaning as in Division 4A.

digital evidence access order (organised crime) means an order issued under section 76AZB(3).

organised crime offence—see section 76AS.

serious offence means the following offences—

(a) an aggravated circumstances offence within the meaning of the *Crimes Act 1900*, section 195,

(b) an offence against the *Crimes Act 1900*, section 55 or 86, Part 3, Division 15, Part 3A, Division 5, Part 4, Division 2, section 99 or 192E or Part 4AC,

(c) an offence against the *Firearms Act 1996*, section 7 or 7A,

(d) an offence against the *Public Health (Tobacco) Act 2008*, section 6(1) or 7(1),

(e) another offence prescribed by the regulations.

specified person, for a digital evidence access order (organised crime), means a person specified in the order as being subject to a direction under the order.

76AS Meaning of "organised crime offence"

(1) In this division, ***organised crime offence*** means a serious offence that is linked to organised crime.

(2) Without limiting subsection (1), a serious offence may be linked to organised crime if the serious offence—

(a) is committed by 2 or more persons, or

(b) involves substantial planning and organisation, or

(c) involves systemic and continuing activity, or

(d) is committed to obtain profit, power or influence, or

(e) is committed for the purpose of retribution against another person or group of persons.

Subdivision 2 Applications for digital evidence access orders (organised crime)

76AT General matters for applications for digital evidence access orders (organised crime)

(1) A police officer may apply for a digital evidence access order (organised crime) in relation to a computer that has been lawfully seized by a police officer other than in connection with the following—

(a) a search warrant within the meaning of Division 4A,

(b) a crime scene warrant.

(2) An application for a digital evidence access order (organised crime) may be made only if the police officer reasonably suspects data contained on the computer is connected to or relevant to the investigation of an organised crime offence.

(3) An application for a digital evidence access order (organised crime) may be made—

(a) within 14 days after the computer is lawfully seized, or

(b) on a later date, but only if the police officer applying for the order demonstrates that it was not reasonably practicable to apply within 14 days.

76AU Applications for digital evidence access orders (organised crime) in person

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

(2) An application for a digital evidence access order (organised crime) 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 (organised crime) 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 (organised crime).

76AV Applications for digital evidence access orders (organised crime) by email or other electronic means

(1) An application for a digital evidence access order (organised crime) 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 (organised crime) 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 (organised crime) 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 (organised crime).

(5) The requirement under subsection (3)(a) 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 digital evidence access order (organised crime) on an application made under this section, the eligible issuing officer may—

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

(b) give the signed order to the applicant in another way prescribed by the regulations.

76AW Applications for digital evidence access orders (organised crime) by telephone

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

(a) in person under section 76AU, or

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

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

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

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

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

(3) If it is not practicable for an application for a digital evidence access order (organised crime) 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 (organised crime) on an application made by telephone must—

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

(b) either—

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

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

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

(a) complete a form of digital evidence access order (organised crime) in the terms indicated by the eligible issuing officer under subsection (4)(b)(ii), and

(b) write on the order—

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

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

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

(7) A digital evidence access order (organised crime) 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.

76AX Information in applications for digital evidence access orders (organised crime)

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

(a) the name of the applicant,

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

(c) a description of the computer,

(d) how and when the computer was obtained by a police officer,

(e) details of the organised crime offence in relation to which it is proposed the digital evidence access order (organised crime) will be issued, including information about how the serious offence is linked to organised crime,

(f) why the person the subject of the application is reasonably suspected of—

(i) committing the organised crime offence, or

(ii) having knowledge of the organised crime offence,

(g) particulars of the grounds on which the application is based, including the grounds for reasonably suspecting data contained on the computer is connected to or relevant to the investigation of an organised crime offence,

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

(i) other information required by the regulations.

(2) If the person the subject of the application for the digital evidence access order (organised crime) is less than 18 years of age, 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 (organised crime) is being sought.

(4) Nothing in this section requires an applicant for a digital evidence access order (organised crime) 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.

76AY False or misleading information in applications

(1) A person must not, in or in connection with an application for a digital evidence access order (organised crime), 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.

76AZ Further application for digital evidence access order (organised crime) after refusal

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

Subdivision 3 Determining applications for digital evidence access orders (organised crime)

76AZA Matters to be considered in determining reasonable grounds for digital evidence access orders (organised crime)

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

76AZB Decisions about applications for digital evidence access orders (organised crime)

(1) The eligible issuing officer must—

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

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

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

(a) there are reasonable grounds for believing the computer was lawfully seized, and

(b) there are reasonable grounds for suspecting data contained on the computer is connected to or relevant to the investigation of an organised crime offence, and

(c) there are reasonable grounds to suspect the person in relation to whom it is proposed the digital evidence access order (organised crime) will be issued—

(i) committed the organised crime offence, or

(ii) has knowledge of the organised crime offence, and

(d) the person in relation to whom it is proposed the digital evidence access order (organised crime) 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 (organised crime) to the applicant.

Subdivision 4 Issue of digital evidence access orders (organised crime)

76AZC Form of digital evidence access orders (organised crime)

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

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

76AZD Term of digital evidence access order (organised crime)

(1) A digital evidence access order (organised crime) remains in force for a period of 7 business days after the order is issued.

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

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

76AZE Effect of digital evidence access order (organised crime)

(1) The executing officer for a digital evidence access order (organised crime) 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 secured by biometric means, including, for example, fingerprints or retina scans.

(3) Without limiting this section, a direction may specify a time by which the specified person is required to carry out the direction.

(4) The executing officer must not direct a specified person who is less than 18 years of age unless reasonable steps are taken to have a suitable person present

to represent the interests of the specified person while the specified person is directed.

(5) To avoid doubt—

(a) information given 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 the taking of identification particulars from persons in custody and other offenders, including section 136, which provides for identification particulars of children who are less than 14 years of age.

(6) In this section—

suitable person, for a specified person, means a person, other than a police officer, who—

(a) is acceptable to the specified person, and

(b) is—

(i) a parent or guardian of the specified person, or

(ii) capable of representing the interests of the specified person.

76AZF Duty to produce digital evidence access order (organised crime)

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

76AZG Failure to comply with digital evidence access order (organised crime)

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

(a) fail to comply with a direction given, in accordance with the digital evidence access order (organised crime), 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 7 years, or both.

(2) Without limiting subsection (1), it is not a reasonable excuse for a specified person for a digital evidence access order (organised crime) 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

76AZH Record of proceedings before eligible issuing officer

(1) An eligible issuing officer who issues a digital evidence access order (organised crime) 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 order.

(2) An eligible issuing officer who refuses to issue a digital evidence access order (organised crime) 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 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 that 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.

76AZI Defects in digital evidence access orders (organised crime)

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

[10] Section 238 Regulations

Omit "digital evidence access orders" wherever occurring in section 238(3).

Insert instead "digital evidence access orders (warrant) and digital evidence access orders (organised crime)".

Schedule 3 Amendment of Criminal Procedure Act 1986 No 209

[1] Schedule 1 Indictable offences triable summarily

Omit “section 76AO” from Table 2, clause 10J.

Insert instead “section 76AO(1) or 76AZG(1)”.

[2] Schedule 1, Table 2, clause 27A

Insert after clause 27—

27A Crime Commission Act 2012

An offence under the *Crime Commission Act 2012*, section 25, 37(3), 45(3), 45A(6), 47D(5) or 47G(1).

Schedule 4 Amendment of Road Transport Act 2013 No 18

[1] Section 271A

Omit the section.

Insert instead—

271A Participation by authorised government agencies in face matching services

(1) An authorised government agency may enter into an arrangement, by agreement, understanding or otherwise, to facilitate participation in a face matching service.

(2) An authorised government agency may do the following—

(a) collect face-matching service information for an authorised purpose,

(b) use face-matching service information for an authorised purpose,

(c) release or disclose face-matching service information to a participant or the Commonwealth—

(i) for the purpose of the participant or the Commonwealth participating in the national agreement, or

(ii) for another purpose in accordance with the national agreement or the Commonwealth Act.

(3) The *Privacy and Personal Information Protection Act 1998* does not apply to the extent of an inconsistency with this section.

(4) The regulations may provide for further matters to facilitate participation in a face matching service.

(5) In this section—

authorised government agency means the following—

(a) TfNSW,

(b) an agent of TfNSW,

(c) another government agency participating in a face matching service in accordance with—

(i) the national agreement, or

(ii) the Commonwealth Act.

authorised purpose, for an authorised government agency, means—

(a) for the purpose of a face matching service, or

(b) another lawful purpose in connection with the exercise of the authorised government agency's functions.

collect includes download.

Commonwealth Act means the *Identity Verification Services Act 2023* of the Commonwealth.

face matching service has the same meaning as in the national agreement.

Face Matching Service Hub has the same meaning as in the Commonwealth Act.

Note— See the Commonwealth Act, section 5.

face-matching service information has the same meaning as in the Commonwealth Act.

Note— ***Face-matching service information*** includes any information that is included in a driver licence or otherwise associated with a driver licence and information included in a document that is issued by a State or Territory in a name of an individual, contains a photograph of the individual and can be used to prove the individual's identity, including a "proof of age" card. See the Commonwealth Act, section 6(2)(g) and (h).

national agreement means the Intergovernmental Agreement on Identity Matching Services entered into by the Commonwealth, the States and the Territories in October 2017, as in force from time to time.

NDLFRS has the same meaning as in the Commonwealth Act.

Note— NDLFRS is short for National Driver Licence Facial Recognition Solution and has the meaning given by the Commonwealth Act, section 5.

release includes—

(a) upload to the NDLFRS, and

(b) relay electronic communications using the Face Matching Service Hub.

Schedule 5 Amendment of Roads Act 1993 No 33

[1] Section 250A Approved camera recording devices—toll offences

Omit section 250A(4)–(5A).

[2] Part 15B

Insert after section 261B—

Part 15B Collection, storage and disclosure of toll camera images

261C Definitions

In this part—

approved toll camera has the same meaning as in section 250A.

photograph has the same meaning as in section 250A.

relevant information means information acquired in the exercise of functions in connection with the use or operation of an approved toll camera, including a photograph taken by an approved toll camera under section 261D.

serious indictable offence has the same meaning as in the *Crimes Act 1900*.

toll camera image means a photograph taken by an approved toll camera.

261D Photographs approved toll camera is permitted to take

An approved toll camera is permitted to take a photograph of the following—

(a) a vehicle,

(b) the driver of a vehicle,

(c) a passenger in a vehicle, including a passenger who is less than 16 years of age.

261E Prohibition on collection, storage and disclosure of toll camera images except for certain purposes

A person who acquires relevant information must not directly or indirectly make a record of, or make use of or disclose, the relevant information except as follows—

(a) in the exercise of functions in connection with—

(i) the payment and collection of tolls, or

(ii) another function prescribed in relation to tolls,

(b) in the exercise of functions in connection with the enforcement of this Act or the regulations under this Act,

(c) as permitted under section 261F or 261G.

Maximum penalty—50 penalty units.

261F Collection, storage and disclosure of toll camera images for purposes relating to NSW Police Force

A person may collect, store and disclose relevant information—

(a) for the investigation of serious indictable offences by the NSW Police Force and the prosecution of the serious indictable offences, or

(b) if it is reasonably necessary to locate a person who the NSW Police Force has been notified is missing, or

(c) to prevent or lessen a serious threat to the life, or health or safety, of a person, including a child, or

(d) to support an investigation into a death, suspected death, fire or explosion for the purposes of the *Coroners Act 2009*.

261G Disclosure of toll camera images to other authorised agencies

(1) A person may disclose relevant information to an authorised agency if—

(a) either or both of the following apply—

(i) the person is—

(A) a toll operator, or

(B) an officer of a toll operator, or

(C) a person exercising functions on behalf of or otherwise acting under the authority of a toll operator,

(ii) the disclosure of the information is in accordance with a protocol approved by the Privacy Commissioner, and

(b) the relevant information was acquired in relation to a vehicle driven in contravention of a requirement to pay a relevant toll.

(2) In this section—

authorised agency means the following persons or agencies—

(a) the Australian Crime Commission,

(b) the Independent Commission Against Corruption,

(c) the New South Wales Crime Commission,

(d) the NSW Police Force,

(e) the Ombudsman,

(f) another person or government agency prescribed for the purpose of this paragraph.