Explanatory Statement

Issued by authority of the Attorney-General

Telecommunications (Interception and Access) Act 1979

Telecommunications (Interception and Access) (Enforcement Agency – NSW Department of Communities and Justice) Declaration 2024

1. The Telecommunications (Interception and Access) (Enforcement Agency – NSW Department of Communities and Justice) Declaration 2024 (the Declaration) is made under paragraphs 176A(3)(a) and (b) of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

2. The TIA Act protects the content of telecommunications and telecommunications data and creates a legal framework for intelligence and law enforcement agencies to access information held by telecommunications providers for law enforcement and national security purposes.

Enforcement agencies

3. Section 176A of the TIA Act defines an enforcement agency for the purposes of being able to access historic telecommunications data as follows:

    a. the agencies that also fall under the definition of 'criminal law-enforcement agency' under section 110A of the TIA Act. These include all state and territory police agencies, the Department of Home Affairs (for limited purposes), the Australian Competition and Consumer Commission, the Australian Securities and Investments Commission, the Australian Criminal Intelligence Commission, and various integrity and corruptions Commissions, and

    b. an authority or body for which a declaration under subsection 176A(3) is in force.

Telecommunications data

4. Telecommunications data is information about a communication – such as the phone numbers of the people that called each other, how long they talked to each other, the email address from which a message was sent and the time the message was sent. Importantly, telecommunications data does not include the content of a communication, such as the subject line of an email or the contents of an SMS.

5. Sections 187A and 187AA of the TIA Act require providers to retain the following telecommunications data for a period of two years:

    a. the subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service

    b. the source of a communication

    c. the destination of a communication

d. the date, time and duration of a communication, or of its connection to a relevant service

e. the type of a communication or of a relevant service used in connection with a communication, and

f. the location of equipment, or a line, used in connection with a communication.

Purpose of the Declaration

6. The purpose of the Declaration is to declare the New South Wales Department of Communities and Justice (NSW Communities and Justice) to be an enforcement agency under subsection 176A(3) of the TIA Act to allow Corrective Services NSW to access telecommunications data.

Legislative scheme

7. Subsections 178(1) and 179(1) of the TIA Act provide that sections 276, 277 and 278 of the *Telecommunications Act 1997* (Telecommunications Act) do not prevent a disclosure of telecommunications data from a service provider should an appropriate authorisation under subsections 178(2) and 179(2) respectively be in place.

8. Subsections 178(2) and 179(2) of the TIA Act allow for an authorised officer of an enforcement agency to authorise the disclosure of specified information or documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

9. Paragraphs 176A(3)(a) and (b) of the TIA Act provide that the Attorney-General may, by legislative instrument, declare that an authority or body is an enforcement agency, and, that persons or kinds of persons specified in a declaration are officers of the enforcement agency, for the purposes of the Act.

10. Subsection 176A(6) of the TIA Act provides that the declaration may be subject to conditions.

Requirements

11. Section 176A of the TIA Act sets out the considerations and requirements for the Attorney-General to make a declaration.

Functions of the agency

12. Under subsection 176A(3B) of the TIA Act, the Attorney-General must not make a make a declaration under subsection 176A(3) of the TIA Act, unless satisfied on reasonable grounds that the functions of the authority or body include:

(a) enforcement of the criminal law; or

(b) administering a law imposing a pecuniary penalty; or

(c) administering a law relating to the protection of the public revenue.

13. The Attorney-General is satisfied the functions of NSW Communities and Justice include the enforcement of the criminal law. NSW Communities and Justice administers the *Crimes (Administration of Sentences) Act 1999* (NSW) which includes criminal penalties under Part 13A for offences such as the trafficking of prohibited goods and the possession of mobile phones in correctional facilities. NSW Communities and Justice also plays a critical role in the detection, investigation and prosecution of offences under the *Crimes Act 1900* (NSW) including offences relating to escaping from lawful custody and threatening witnesses, as well as terrorism offences under the *Terrorism (High Risk Offenders) Act 2017* (NSW) and the *Criminal Code Act 1995* (Cth).

14. Paragraph 176A(4)(b) of the TIA Act requires the Attorney-General to have regard to whether having access to telecommunications data would be reasonably likely to assist NSW Communities and Justice perform its functions of enforcing the criminal law.

15. Illicit mobile telephones pose a particular threat within correctional facilities. They are used to organise escape attempts, threaten the safety of victims and witnesses, organise trafficking of contraband, and facilitate behaviour contrary to national security interests. Telecommunications data is particularly vital in establishing the ownership or location of mobile phones used to commit offences within correctional facilities and therefore would assist NSW Communities and Justice in the performance of its functions.

16. Acknowledging this, the *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Comprehensive Review) recommended that corrective services agencies have access to telecommunications data if their respective state or territory government considered it necessary.

Privacy considerations

17. Paragraph 176A(4)(c) of the TIA Act requires the Attorney-General to have regard to protection of personal information by the authority or body.

18. Subparagraph 176A(4)(c)(i) of the TIA Act requires consideration of whether the agency is required to comply with the Australian Privacy Principles. As a NSW Government entity, NSW Communities and Justice is not required to comply with the Australian Privacy Principles.

19. However, NSW Communities and Justice is required to comply with a binding scheme that provides for the protection of personal information through the *Privacy and Personal Information Protection Act 1998* (NSW) (NSW Privacy Act) and the *Crimes (Administration of Sentences) Act 1999* (NSW).

20. The NSW Information Protection Principles, under the NSW Privacy Act, are broadly comparable to the Australian Privacy Principles in providing safeguards for the collection, use, disclosure and security of personal information. Although there are differences, NSW Communities and Justice has agreed, in line with subparagraph 176A(4)(c)(iii) of the TIA Act, to a scheme that reflects the requirements outlined in subsection 176A(4A).

21. Firstly, the scope of personal information under the NSW Privacy Act is limited and does not explicitly include telecommunications data. This has been addressed as NSW Communities and

Justice, through its Privacy Impact Assessment, has accepted that telecommunications data is personal information and has undertaken to treat it as such under all relevant legislation.

22. Secondly, telecommunications data obtained through the use of a journalist information warrant would not be personal information under the NSW Privacy Act and would not be protected by the NSW Information Protection Principles. However, as it is not necessary for NSW Communities and Justice to seek journalist information warrants in order to address illicit mobile telephone use in correctional facilities, doing so is explicitly prevented by paragraph 4(1)(b) of the Declaration.

23. The *Privacy and Personal Information Protection Amendment Act 2022* (NSW) (PIPP Act) amended the NSW Privacy Act to create a Mandatory Notification of Data Breaches Scheme to require public sector agencies bound by the PPIP Act to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information likely to result in serious harm. Agencies also have to make reasonable attempts to mitigate the harm done by a data breach, maintain an internal data breach incident register, and have a publicly accessible data breach policy. These changes came into effect on 28 November 2023.

24. As set out in its Privacy Management Plan, all areas of NSW Communities and Justice must report all data breaches or allegations of a breach to the Open Government, Information and Privacy Unit, which determines whether a breach should be reported to the Privacy Commissioner.

25. As a law enforcement agency for the purposes of the NSW Privacy Act, NSW Communities and Justice is exempt from a number of the NSW Information Protection Principles. Further, NSW Communities and Justice is not required to, and does not, comply with other of the Principles due to the nature of its role and the information it will be collecting. However, these exemptions or areas of non-compliance are commensurate with exemptions under the Australian Privacy Principles for enforcement agencies.

26. For the purposes of paragraph 176A(4A)(b) of the TIA Act, NSW Communities and Justice will voluntarily report on the collection and use of telecommunications data to the NSW Privacy Commissioner and the NSW Minister for Corrections. This is in addition to the oversight of the use of telecommunications data by the Commonwealth Ombudsman as set out in Chapter 4A of the TIA Act.

27. For the purposes of paragraph 176A(4A)(c) of the TIA Act, sections 45 and 53 of the NSW Privacy Act provide a mechanism for an individual to make a complaint to the NSW Privacy Commissioner about an alleged breach of privacy by a public sector agency or may seek internal review by the agency. This process is overseen by the NSW Civil and Administrative Appeals Tribunal.

Compliance with TIA Act obligations

28. Paragraph 176A(4)(d) of the TIA Act requires the Attorney-General to have regard to whether NSW Communities and Justice proposes to adopt processes and practices to ensure it complies with its obligations under Chapter 4 of the TIA Act.

29. To meet its obligations, NSW Communities and Justice has:

- a purpose-built electronic data storage system for intelligence-related and other protected and sensitive information, accessible only by authorised staff and which keeps sufficient records for oversight purposes
- a clear hierarchy of approval before consent is given to make an authorisation under the TIA Act
- clearly defined processes to record authorisation requests, outcomes, and use of information obtained, and
- training on data retention laws, including authorised officer considerations.

30. NSW Communities and Justice systems will continue to report on its use of telecommunications data to the Commonwealth Attorney-General, the NSW Attorney General, the NSW Minister for Corrections, the Office of the Commonwealth Ombudsman (OCO) and the NSW Privacy Commissioner, as required by the TIA Act and NSW legislation.

31. Further, the OCO has assessed NSW Department of Communities and Justice's systems, policies and processes to ensure Corrective Services NSW can appropriately deal with and protect telecommunications data as required by the TIA Act.

32. As set out in the OCO's annual report on inspections during 2022–23, NSW Department of Communities and Justice's framework for using telecommunications data contained appropriate detail to support use of the powers. NSW Department of Communities and Justice was also assessed as having a 'maturing' to 'mature' compliance culture with respect to using telecommunications data powers.

Public interest

33. Paragraph 176A(4)(e) of the TIA Act requires the Attorney-General to have regard to whether the declaration would be in the public interest. The importance of telecommunications data to the functions of NSW Communities and Justice, the crucial role that NSW Communities and Justice plays in enforcing the criminal law and protecting public safety and the privacy and other protections that NSW Communities and Justice has in place mean that providing NSW Communities and Justice access to telecommunications data is in the public interest.

Consultation

34. The Office of Impact Analysis (the OIA) has advised that a Regulation Impact Statement is not required. The OIA consultation reference number is **OBPR23-03901**.

35. The Declaration is an instrument subject to disallowance under section 42 of the *Legislation Act 2003* and therefore a Statement of Compatibility with Human Rights has been provided at **Attachment A**.

36. The Attorney-General's Department consulted closely with NSW Communities and Justice, the Office of the Australian Information Commissioner and the Office of the Commonwealth Ombudsman on this Declaration.

Details of the Telecommunications (Interception and Access) (Enforcement Agency – NSW Department of Communities and Justice) Declaration 2024

37. The Attorney-General's Declaration is made under the authority of paragraphs 176A(3)(a) and (b) of the TIA Act.

38. Section 1 sets out the name of the Declaration.

39. Section 2 provides for the commencement of the Declaration, being the day after registration on the Federal Register of Legislation.

40. The note following section 2 refers to paragraph 176A(10)(b) of the TIA Act which provides that the declaration will cease to be in force at the end of the period of 40 sitting days of a House of the Parliament after the Declaration comes into force. This reflects the temporary nature of these declarations.

41. In subsection 3(1) of the Declaration, the Attorney-General declares NSW Communities and Justice to be an enforcement agency under paragraph 176A(3)(a) of the TIA Act.

42. In subsection 3(2) of the Declaration, the Attorney-General declares each staff member of that part of New South Wales Department of Communities and Justice known as Corrective Services NSW to be officers of New South Wales Department of Communities and Justice for the purposes of the TIA Act.

43. The declaration in section 3 is subject to two conditions which are set out in section 4 of the instrument.

44. Subsection 176A(6) of the TIA Act provides that the declaration of an enforcement agency may be subject to conditions. Subsection 176A(7) of the TIA Act provides that a condition may provide that the authority or body is not to exercise a power conferred on an enforcement agency by or under a specified provision in Chapter 4. The authority or body is taken not to be an enforcement agency for the purposes of that provision.

45. Paragraph 4(1)(a) of the Declaration provides that the declaration is only in relation to that part of NSW Communities and Justice that is known as Corrective Services NSW. No other part of NSW Communities and Justice will be able to access telecommunications data. This approach to the declaration is needed because Corrective Services NSW is not a standalone authority or body in its own right, as contemplated by section 176A of the TIA Act.

46. Paragraph 4(1)(b) of the Declaration provides that NSW Communities and Justice is not to exercise the power under section 180Q of the TIA Act (that is, apply for journalist information warrants). The note following paragraph 4(1)(b) clarifies that NSW Communities and Justice is taken not to be an enforcement agency for the purposes of section 180Q of the TIA Act.

47. NSW Communities and Justice has not been provided the ability to exercise the power under section 180Q of the TIA Act because telecommunications data obtained through the use of a journalist information warrant may not be protected by the NSW Information Protection Principles. NSW Communities and Justice has agreed that access to this information is not necessary for the performance of its functions and has agreed to this condition.

Attachment A

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Telecommunications (Interception and Access) (Enforcement Agency – NSW Department of Communities and Justice) Declaration 2024

The *Telecommunications (Interception and Access) (Enforcement Agency – NSW Department of Communities and Justice) Declaration 2024* (the Declaration) is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011.*

Overview of the legislative instrument

Section 176A of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) defines an enforcement agency for the purposes of being able to access historic telecommunications data.

Section 176A of the TIA Act defines an enforcement agency for the purposes of being able to access historic telecommunications data as follows:

- the 20 agencies that also fall under the definition of 'criminal law-enforcement agency' under section 110A of the TIA Act. These include all state and territory police agencies, the Department of Home Affairs (for limited purposes), the Australian Competition and Consumer Commission, the Australian Securities and Investments Commission, the Australian Criminal Intelligence Commission, and various integrity and anti-corruption Commissions, and
- an authority or body for which a declaration under subsection 176A(3) is in force.

The Declaration is a legislative instrument made by the Attorney-General under subsection 176A(3) of the TIA Act, and declares New South Wales Department of Communities and Justice (NSW Communities and Justice) to be an enforcement agency under subsection 176A(3) of the TIA Act to allow access to telecommunications data. Additionally, the Declaration specifies each staff member of NSW Communities and Justice to be officers under the TIA Act.

The Declaration is subject to two conditions:

- the declaration is only in relation to that part of NSW Communities and Justice known as Corrective Services NSW, and
- NSW Communities and Justice is not to exercise the power in section 180Q of the TIA Act.

As such, this Declaration allows only the relevant part of NSW Communities and Justice the ability to access historic telecommunications data.

The Declaration does not change the statutory basis on which enforcement agencies are able to access telecommunications data and does not amend the existing processes for lawfully accessing telecommunications data.

Human rights implications

The Declaration engages the right to privacy under Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) on the basis that the telecommunications data retained pursuant to subsection 187A(1) of the TIA Act will be accessible by NSW Communities and Justice in accordance with the existing lawful access provisions in the Act.

Article 17 provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation, and that everyone has the right to the protection of the law against such interference or attacks.

The protection against arbitrary or unlawful interference with privacy under Article 17 can be permissibly limited in order to achieve a legitimate objective and where the limitations are lawful and not arbitrary. The term *unlawful* in Article 17 of the ICCPR means that no interference can take place except as authorised under domestic law. Additionally, the term arbitrary in Article 17(1) of the ICCPR means that any interference with privacy must be in accordance with the provisions, aims and objectives of the ICCPR and should be reasonable in the particular circumstances.[1] The United Nations Human Rights Committee has interpreted *reasonableness* to mean that any limitation must be proportionate and necessary in the circumstances.

The Declaration limits the right to privacy as it allows access to telecommunications data as authorised under domestic law – namely the existing provisions in the TIA Act. However, it is reasonable in the particular circumstances as it is proportionate and necessary.

In considering the second component (that is, reasonableness) consideration has been given to the:

- functions of NSW Communities and Justice and whether they necessitate access to telecommunications data, and
- privacy and other safeguards in place to minimise the privacy impacts on any persons to whom the data relates or is appreciably linked to.

Functions of NSW Communities and Justice

As set out in the conditions, the Declaration only relates to the part of NSW Communities and Justice known as Corrective Services NSW (CSNSW), which performs the functions of a corrective services agency and enforces the criminal law.

Specifically, NSW Communities and Justice administers the *Crimes (Administration of Sentences) Act 1999* (NSW) which includes criminal penalties under Part 13A for offences such as the trafficking of prohibited goods and the possession of mobile phones in correctional facilities. NSW Communities and Justice also plays a critical role in the detection, investigation and prosecution of offences under the *Crimes Act 1900* (NSW) including offences relating to escaping from lawful custody and threatening witnesses as well as terrorism offences under the *Terrorism (High Risk Offenders) Act 2017* (NSW) and the *Criminal Code Act 1995* (Cth).

[1] *Toonen v Australia*, Communication No. 488/1992, U.N. Doc CCPR/C/50/D/488/1992 (1994) at 8.3.

The Declaration addresses the legitimate objectives of national security, public order and the rights of others. Illicit mobile telephones pose a particular threat within correctional facilities. They are used to organise escape attempts, threaten the safety of victims and witnesses, organise trafficking of contraband, as well as facilitate behaviour contrary to national security interests. Telecommunications data is particularly vital in establishing the ownership or location of mobile phones used to commit offences within correctional facilities. Access to this data would assist NSW Communities and Justice to better identify, investigate and prevent illicit mobile phone-related crime in correctional facilities, ensuring any criminal offences are appropriately detected and prosecuted, mitigating the risk posed to national security and public order.

Parliamentary Joint Committee on Human Rights (PJCHR) commentary

On 14 June 2023, the PJCHR raised concerns about the human rights impact of previous CSNSW declarations (Report 6 of 2023). On 3 August 2023, in Report 8 of 2023, the PJCHR further scrutinised aspects of the previous declaration for CSNSW. The PJCHR expressed a view that:

- CSNSW has not demonstrated a pressing and substantial issue of public or social concern
- CSNSW has not accessed telecommunications frequently enough to justify limiting individuals' right to privacy
- CSNSW previously accessed telecommunication data via NSW Police, and other corrective services are still doing this successfully, therefore the necessity of this power has not been established for CSNSW, and
- the scope of officers who may access to telecommunications data is too broad. As a matter of law, any of the over 10,000 officers within CSNSW could be authorised to access this private telecommunications data.

In resonse to the specific concerns articulated by the PJCHR, the NSW Government has advised:

- There is a public expectation that CSNSW will keep the community safe by effectively administering sentences imposed by the courts. This includes not only securely holding offenders, and disrupting offending within correctional centres, but seeking to identify and treat inmates' criminogenic needs in order to reduce reoffending.
- The number of times telecommunications data has been accessed does not necessarily reflect its operational and safety value. Use of this power correlates directly to illegal (or suspected) activity by staff and inmates. There may be periods where such activity is minimal and can be addressed by existing, and less intrusive, search and intelligence capacity. Conversely, there may be periods where such activity is high in volume, cannot be supported by existing intelligence capacity and access to telecommunications data may be required.
- CSNSW is best-placed to determine the relevance of data and other information associated with inmates and offenders under its management because NSW Police lacks this operational context. It is impractical and presumptuous to rely on NSW Police to obtain telecommunications data for CSNSW, noting the very high volume, nature and complexity of NSW Police's own law enforcement functions. CSNSW has a demonstrated capacity and expertise to undertake these functions in-house.
- In practice, access to telecommunications data powers within CSNSW is strictly limited. Only six executive-level officers can make authorisations, and only officers within defined organisational units, who have been provided with specific access and training, are able to access the data. Once telecommunications data is received, it is held in a secure web-based system that is only accessible by select personnel and is fully auditable.

Other privacy safeguards

NSW Communities and Justice is subject to NSW privacy laws including the *Privacy and Personal Information Protection Act 1998* (NSW), and secrecy provisions including in the *Crimes (Administration of Sentences) Act 1999* (NSW). Importantly, the privacy protections under NSW legislation are similar to those set out in the *Privacy Act 1988* (Cth). These protections are complemented by the strict requirements of the TIA Act for the collection, use and disclosure of information obtained by law enforcement agencies.

Oversight and reporting requirements under the TIA Act also provide accountability on the use of telecommunications data by NSW Communities and Justice. NSW Communities and Justice will be subject to independent oversight by the Commonwealth Ombudsman, who will inspect the records of NSW Communities and Justice to determine the extent of its (and its officers) compliance with Chapter 4 of the TIA Act and the Ombudsman will also report annually to the Attorney-General about the results of those inspections. The Attorney-General also reports to Parliament on the operation of the data retention scheme each year as required by section 187P of the TIA Act.

NSW Communities and Justice will be excluded from obtaining Journalist Information Warrants under section 180Q of the TIA Act, as these warrants are not relevant to its functions or the objectives of addressing illicit mobile telephone crime in correctional facilities.

In addition, the Declaration is proportionate and the least rights restrictive option. NSW Communities and Justice has in place processes and systems that ensure telecommunications data will only be accessed when required and will be appropriately protected.

NSW Communities and Justice systems also allow it to report on its use of telecommunications data to the Commonwealth Attorney-General, the NSW Attorney General, the NSW Minister for Corrections and the NSW Privacy Commissioner as required by the TIA Act and NSW legislation.

Conclusion

This Declaration is made for the legitimate purpose of protecting national security, public order and the rights of others. The Declaration is compatible with human rights as set out above, and to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate.