Explanatory Statement

Issued by authority of the Attorney-General

Telecommunications (Interception and Access) Act 1979

Telecommunications (Interception and Access) (Criminal Law-Enforcement Agency – ACT Integrity Commission) Declaration 2024

1. The Telecommunications (Interception and Access) (Criminal Law-Enforcement Agency – ACT Integrity Commission) Declaration 2024 (the Declaration) is made under paragraphs 110A(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 110A of the TIA Act defines a criminal law-enforcement agency, which is able to access stored communications and telecommunications data, as follows:

    a. The Australian Federal Police, 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 corruption Commissions, and

    b. an authority or body for which a declaration under subsection 110A(3) is in force.

Stored communications

4. 'Stored communications' refers to the content of messages and emails sent via telecommunications systems which are stored by a telecommunications provider, for example, on a server or hard drive. They are not accessible by anyone except a party to the communication without the assistance of the telecommunications provider.

5. Division 2 of Part 3-3 of Chapter 3 of the TIA Act provides that a criminal law-enforcement agency may apply for a stored communications warrant in order to access material held by a carrier. Division 2 of Part 3-1A of Chapter 3 provides for an issuing agency (which includes a criminal law-enforcement agency) to issue a domestic preservation notice, which requires the telecommunications provider to preserve all stored communications relevant to the notice for a specified period of time.

Telecommunications data

6. 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. Telecommunications data does

not include the content of a communication, such as the subject line of an email or the contents of an SMS.

7. 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

8. The purpose of the Declaration is to declare the ACT Integrity Commission to be an criminal law-enforcement agency under subsection 110A(3) of the TIA Act to enable it to access stored communications and telecommunications data.

Legislative scheme

9. Paragraphs 110A(3)(a) and (b) of the TIA Act provide that the Attorney-General may, by legislative instrument, declare that an authority or body is a criminal law-enforcement agency, and that persons or kinds of persons specified in a declaration are officers of the criminal law-enforcement agency for the purposes of the Act.

10. Subsection 110A(6) of the TIA Act provides that the declaration may be subject to conditions.

Considerations

11. Section 110A of the TIA Act sets out the considerations for the Attorney-General to make a declaration.

Functions of the agency

12. Under subsection 110A(3B) of the TIA Act, the Attorney-General must not make a declaration under subsection 110A(3), unless satisfied on reasonable grounds that the functions of the authority or body include the investigation of a 'serious contravention'.

13. The Attorney-General is satisfied the functions of the ACT Integrity Commission include the investigation of serious contraventions as defined in section 5E of the TIA Act. The ACT Integrity Commission is responsible for investigating alleged and actual serious and systemic corrupt conduct within the ACT public sector. This conduct includes conduct which is criminal

in nature and which carries significant criminal penalties under Territory and Commonwealth law, such as theft, fraud and bribery relating to an ACT public official. The ACT Integrity Commission also plays a role in providing support for the prosecution of these crimes by Territory and Commonwealth prosecution authorities by referring matters throughout the investigation process.

14. Paragraph 110A(4)(b) of the TIA Act requires the Attorney-General to have regard to whether having access to stored communications would be reasonably likely to assist the ACT Integrity Commission to perform its function of investigating serious contraventions.

15. The ability to access stored communications and telecommunications data will assist the ACT Integrity Commission in its role of investigating allegations of serious and systemic corrupt conduct through increased capacity to gather and analyse relevant information, and pursue search warrants and surveillance device warrants. Stored communications and telecommunications data is an important tool in seeking to identify, investigate and disrupt potentially corrupt behaviour within the ACT public sector.

Privacy considerations

16. Paragraph 110A(4)(c) of the TIA Act requires the Attorney-General to have regard to protection of personal information by the authority or body.

17. This includes consideration of whether the agency is required to comply with the Australian Privacy Principles (APPs) or a binding scheme that provides protection of personal information, comparable to the APPs.

18. As an ACT Government entity, the ACT Integrity Commission is not required to comply with the APPs. However, it is required to comply with a binding scheme that provides for the protection of personal information through the *Information Privacy Act 2014* (ACT) (ACT Privacy Act).

19. The ACT Territory Privacy Principles (TPPs), under the ACT Privacy Act, are comparable to the APPs in providing safeguards for the collection, use, disclosure and security of personal information.

Compliance with TIA Act obligations

20. Paragraph 110A(4)(d) of the TIA Act requires the Attorney-General to have regard to whether the ACT Integrity Commission proposes to adopt processes and practices to ensure it complies with its obligations under Chapter 3 of the TIA Act.

21. To meet its obligations, the ACT Integrity Commission has:

- a purpose-built electronic data storage system known as ‘Condor’ for protected and sensitive information, accessible only by authorised staff, 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.

22. The ACT Integrity Commission will report on its use of telecommunications data to the Commonwealth Attorney-General and the Office of the Commonwealth Ombudsman (OCO) as required by the TIA Act.

23. In March 2024 the OCO assessed the ACT Integrity Commission's systems, policies and processes to ensure it can appropriately deal with and protect telecommunications data as required by the TIA Act.

24. In its report, the OCO assessed the ACT Integrity Commission was well-placed to exercise the powers under Chapter 3 and 4 of the TIA Act.

Public interest

25. Paragraph 110A(4)(e) of the TIA Act requires the Attorney-General to have regard to whether the declaration would be in the public interest. Providing the ACT Integrity Commission with access to stored communications and telecommunications data will enhance its ability to investigate, expose and prevent corrupt conduct in the ACT public sector. This will enhance community safety and increase trust and integrity in the ACT public sector.

Consultation

26. The Office of Impact Analysis (the OIA) has advised that a Regulation Impact Statement is not required. The OIA consultation reference number is OIA24-07482.

27. 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**.

28. The Attorney-General's Department consulted the ACT Integrity Commission, the Office of the Australian Information Commissioner and the Office of the Commonwealth Ombudsman in the making of this Declaration.

Details of the Telecommunications (Interception and Access) (Criminal Law-Enforcement Agency—ACT Integrity Commission) Declaration 2024

29. The Declaration is made under the authority of paragraphs 110A(3)(a) and (b) of the TIA Act.

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

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

32. The note following section 2 refers to paragraph 110A(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 the declaration.

33. In subsection 3(1) of the Declaration, the Attorney-General declares the ACT Integrity Commission to be a criminal law-enforcement agency under paragraph 110A(3)(a) of the TIA Act.

34. In subsection 3(2) of the Declaration, the Attorney-General declares each staff member of the ACT Integrity Commission to be officers of the ACT Integrity Commission for the purposes of the TIA Act.

35. Subsection 110A(6) of the TIA Act provides that the declaration of a criminal law-enforcement agency may be subject to conditions. The declaration in section 3 is subject to one condition which is set out in section 4 of the instrument.

36. Paragraph 4(1)(a) of the Declaration provides that ACT Integrity Commission officers are not to exercise powers under the Act with respect to any preliminary inquiries conducted by the ACT Integrity Commission under the authority of section 86 of the *Integrity Commission Act 2018* (ACT).

37. The ACT Integrity Commission has not been declared to exercise TIA Act powers with respect to preliminary investigations at the request of the ACT Government. The restriction on the use of coercive and covert powers during preliminary inquiries is due to their impact on human rights and potential engagement with the *Human Rights Act 2004* (ACT).

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) (Criminal Law-Enforcement Agency—ACT Integrity Commission) Declaration 2024

The *Telecommunications (Interception and Access) (Criminal Law-Enforcement Agency—ACT Integrity Commission) 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 110A of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) defines a criminal law-enforcement agency for the purposes of being able to access stored communications and telecommunications data as follows:

- a list of agencies, including the Australian Federal Police, 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 110A(3) is in force.

The Declaration is a legislative instrument made by the Attorney-General under subsection 110A(3) of the TIA Act, and declares the ACT Integrity Commission to be a criminal law-enforcement agency under subsection 110A(3) of the TIA Act to allow access to stored communications and telecommunications data. Additionally, the Declaration specifies each staff member of the ACT Integrity Commission to be officers under the TIA Act.

The Declaration is subject to one condition:

- ACT Integrity Commission officers are not to exercise powers under the Act with respect to any preliminary inquiries conducted by the ACT Integrity Commission under the authority of section 86 of the *Integrity Commission Act 2018* (ACT).

The Declaration allows the ACT Integrity Commission to exercise powers under Chapters 3 and 4 of the TIA Act with respect to investigations conducted under Part 3.4 of the *Integrity Commission Act 2018* (ACT).

The Declaration does not change the statutory basis on which criminal law-enforcement agencies are able to access stored communications or telecommunications data, and does not amend the existing processes for lawfully accessing that material.

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 stored communications and telecommunications data preserved pursuant to the TIA Act will be accessible by the ACT Integrity Commission 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 stored communications and 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 the ACT Integrity Commission and whether they necessitate access to stored communications and telecommunications data, and
- privacy and other safeguards in place to minimise the privacy impacts on any person to whom the material relates or is appreciably linked to.

Functions of the ACT Integrity Commission

The ACT Integrity Commission performs the functions of an anti-corruption authority and contributes to the enforcement of the criminal law.

Specifically, the ACT Integrity Commission is responsible for investigating alleged and actual serious and systemic corrupt conduct within the ACT public sector. This conduct includes conduct which is criminal in nature and which carries criminal penalties under Territory and Commonwealth law, such as theft, fraud and bribery relating to an ACT public official. The ACT Integrity Commission also plays a role in providing support for the prosecution of these crimes by Territory and Commonwealth prosecution authorities by referring matters throughout the investigation process.

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

In furthering the ACT Integrity Commission's ability to combat corruption, the Declaration addresses the legitimate objectives of national security and public order. Telecommunications data is particularly vital in establishing the ownership or location of mobile phones used to commit criminal offences. Stored communications include the content of messages that may disclose criminal or corrupt conduct. Access to this data would assist the ACT Integrity Commission to better identify, investigate and prevent serious and systemic corrupt conduct within the ACT public sector, ensuring any criminal offences are appropriately detected and prosecuted, mitigating the risk posed to national security and public order.

Other privacy safeguards

The ACT Territory Privacy Principles under the *Information Privacy Act 2004* (ACT) are broadly comparable to the Australian Privacy Principles (APPs) in that they provide safeguards for the collection, use, disclosure and security of personal information.

Oversight and reporting requirements under the TIA Act will provide accountability on the use of stored communications and telecommunications data by the ACT Integrity Commission. The Commission will be subject to independent oversight by the Commonwealth Ombudsman, who will inspect the records of the ACT Integrity Commission to determine the extent of its (and its officers') compliance with Chapters 3 and 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.

The ACT Integrity Commission will be excluded from accessing stored communications and telecommunications data for the purposes of preliminary inquiries under section 86 of the *Integrity Commission Act 2018* (ACT). The ACT Government wishes to restrict the use of coercive and covert powers during preliminary inquiries due to their impact on human rights and potential engagement with the *Human Rights Act 2004* (ACT). The declaration instrument has been drafted in such a way as to give effect to this condition. By requesting restricted access to stored communications and telecommunications data in this way, the ACT Government has demonstrated a commitment to protecting human rights with respect to powers conferred under the TIA Act.

In regards to being proportionate and as least rights-restrictive as possible, the TIA Act requires, and the ACT Integrity Commission has demonstrated, that it has processes and systems in place that ensure stored communications and telecommunications data will only be accessed when required and will be appropriately protected. The ACT Integrity Commission systems also allow the agency to report on its use of stored communications and telecommunications data to the Commonwealth Attorney-General and the Commonwealth Ombudsman as required by the TIA Act.

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.