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) (No. 2) Declaration 2024*

1. The *Telecommunications (Interception and Access) (Criminal Law-Enforcement Agency—ACT Integrity Commission) (No. 2) 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 privacy of telecommunications 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.

Criminal law-enforcement agencies

1. Section 110A of the TIA Act defines ‘criminal law-enforcement agency’, being agencies which are able to access stored communications and telecommunications data under the TIA Act, as follows:
	1. 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
	2. an authority or body for which a declaration under subsection 110A(3) is in force.

Stored communications

1. ‘Stored communications’ refers to the content of communications that are not passing over a telecommunications system, that are stored by a carrier, and that are not accessible by anyone except a party to the communication without the assistance of the telecommunications provider. Examples of stored communications include voicemail messages or emails held by a carrier.
2. 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 also 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

1. Telecommunications data is information about a communication, such as time, date and duration of a communication, or the service or address from which a communication was sent. Telecommunications data does not include the content of a communication, such as the subject line of an email or the content of an SMS.
2. Division 4 of Part 4-1 of Chapter 4 of the TIA Act provides that officers of a criminal law-enforcement agency, being officers of an enforcement agency under section 176A, may authorise disclosure of existing or prospective telecommunications data if satisfied that it is reasonably necessary based on relevant criteria.

Purpose of the declaration

1. The purpose of the declaration is to re-designate the ACT Integrity Commission as a criminal law-enforcement agency under subsection 110A(3) of the TIA Act to enable it to continue to access stored communications and telecommunications data. The ACT Integrity Commission was previously declared to be a criminal law-enforcement agency pursuant to the *Telecommunications (Interception and Access) (Criminal Law-Enforcement Agency—ACT Integrity Commission) Declaration 2024.* That declaration is due to expire on 4 February 2025, based on the proposed sittings for 2025 agreed by the House of Representatives and Senate on 10 October 2024, which is 40 sitting days after its commencement, in accordance with subsection 110A(10) of the TIA Act.

Legislative scheme

1. 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.
2. Subsection 110A(6) of the TIA Act provides that the declaration may be subject to conditions.

Considerations

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

Functions of the agency

1. 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’.
2. 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 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.
3. 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.
4. 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 are important tools for identifying, investigating and disrupting potentially corrupt behaviour within the ACT public sector.

Privacy considerations

1. 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. 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. As an ACT Government entity, the ACT Integrity Commission is not required to comply with the APPs. However, it is required to comply with the Territory Privacy Principles (TPPs) under the *Information Privacy Act 2014* (ACT) (IP Act). These TPPs are directly comparable to the APPs in providing safeguards for the collection, use, disclosure and security of personal information.
2. Subparagraph 110A(4A)(b) requires the comparable scheme to include a mechanism for monitoring compliance with the scheme. Under section 29 of the IP Act the Information Privacy Commissioner has functions that include ‘helping public sector agencies to comply with the TPPs and TPP codes’. Compliance with the TPPs is supported by internal ACTIC procedures for ensuring adherence to the TPPs and responding to privacy breaches, including having staff experienced in working in confidential and/or security-classified environments.
3. Finally, subparagraph 110A(4A)(c) requires that the comparable scheme include a mechanism for individuals to seek recourse if their personal information is mishandled. The Information Privacy Commissioner can investigate privacy complaints under section 29 of the IP Act.

*Compliance with TIA Act obligations*

1. 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.
2. To meet its obligations, the ACT Integrity Commission has:
* a purpose‑built electronic data storage system, 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.
1. The ACT Integrity Commission will continue to report on its use of telecommunications data to the Attorney-General and the Office of the Commonwealth Ombudsman as required by the TIA Act.

Public interest

1. 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

1. The Office of Impact Analysis has advised that an Impact Analysis is not required. The OIA consultation reference number is OIA24-07482.
2. 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**.
3. 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) (No. 2) Declaration 2024

1. The declaration is made under the authority of paragraphs 110A(3)(a) and (b) of the TIA Act.
2. Section 1 sets out the name of the declaration.
3. Section 2 provides for the commencement of the declaration, being 5 February 2025.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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).
9. 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) (No. 2) Declaration 2024***

The *Telecommunications (Interception and Access) (Criminal Law-Enforcement Agency—ACT Integrity Commission) (No. 2) 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]](#footnote-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 because it is proportionate and necessary.

In considering the 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 protections and other safeguards in place to minimise the privacy impacts on any person to whom the material relates or is appreciably linked.

*Functions of the ACT Integrity Commission*

Similar to other integrity and anti-corruption commissions in Australia with permanent access to stored communications and telecommunications data under section 110A of the TIA Act, the ACT Integrity Commission performs the functions of an anti-corruption authority and contributes to the enforcement of the criminal law.

The ACT Integrity Commission is responsible for investigating alleged and actual serious and systemic corrupt conduct within the ACT public sector. This 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.

Serious and systemic corruption have significant detrimental impacts on public administration and can erode trust in the Government, Parliament and democracy. Corruption frequently involves multiple parties, some or all of whom take active steps to conceal their conduct, or the improper purpose driving their conduct. The declaration addresses the legitimate objective of protecting public order, by providing the ACT Integrity Commission with powers required to detect and investigate alleged serious and systemic corrupt conduct within the ACT public sector. The ability to exercise covert investigative and surveillance powers under the TIA Act will enable the Commission to obtain relevant information that would be critical for making findings of fact in relation to corruption issues and making robust recommendations directed at preventing corruption or mitigating against any adverse consequences of corruption. These powers would enable the Commission to access information and data that would not otherwise be available, and may be critical to an investigation.

For example, access to telecommunications data can be essential to establish whether or not parties to alleged serious and systemic corruption are in contact, and can provide foundational evidence that is essential to support applications for further investigative powers such as search warrants. Access to stored communications, such as the content of messages between alleged parties to serious and systemic corruption, can be essential to determine the nature and extent of their conduct. Continued access to these powers will assist the ACT Integrity Commission to better identify, investigate and prevent serious and systemic corrupt conduct within the ACT public sector, ensuring criminal offences are appropriately detected and prosecuted.

As bodies charged with the investigation of corrupt conduct within the public sector, it is important that integrity and anti-corruption bodies are vested with the powers and capabilities they require to effectively discharge their functions, and are not dependant on other agencies—and in particular, on agencies within their jurisdiction—to exercise such powers. While there will be cases where it is appropriate for integrity and anti-corruption bodies to partner with other law enforcement agencies when conducting investigations, the ability for the ACT Integrity Commission and other integrity and anti-corruption bodies to exercise powers under the TIA Act independently is important to:

* ensure that the ACT Integrity Commission and other, similar agencies are able to determine, and exercise powers, in accordance with their own investigative priorities, and
* maintain the confidentiality and integrity of the ACT Integrity Commission and other, similar agencies’ investigations—including, but not limited to, in cases where an investigation relates to the conduct of a law enforcement agency within their jurisdiction.

*Other privacy safeguards*

The ACT Integrity Commission is subject to the ACT Territory Privacy Principles under the *Information Privacy Act 2004* (ACT), which are broadly comparable to the Australian Privacy Principles (APPs). The TPPs 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 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.

Consistent with the approach taken in section 110A for all criminal law-enforcement agencies, the Declaration provides that all staff members of the ACT Integrity Commission will be officers for the purpose of the TIA Act. The declaration of staff members as being ‘officers’ for the purposes of the TIA Act is mechanical in nature, and reflects that the various Commonwealth, state and territory agencies that operate under the TIA Act have different employment arrangements that must be accounted for by defining the range of ‘officers’ of each agency. The declaration of staff members as ‘officers’ for the purposes of the TIA Act does not permit those staff members to exercise powers, such as by applying for stored communications warrants or authorising access to telecommunications data. The TIA Act requires the chief officer of each agency to declare particular officers of their agency for the purpose of exercising particular powers, and imposes appropriate limits on such declarations. For example:

* only officers nominated in writing under subsection 110(3) of the TIA Act who hold an office or position involved in the management of the agency may apply on behalf of the agency for a stored communications warrant, and
* only ‘authorised officers’ holding a management position or office, authorised in writing under section 5B of the TIA Act may exercise powers under Chapter 4 of the Act to authorise access to telecommunications data.

In practice, access to the powers is managed via internal governance structures and procedures, is limited to relevant officers of the agency and is subject to external oversight. 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 Attorney-General and the Commonwealth Ombudsman as required by the TIA Act.

The framework for the authorisation of powers under the TIA Act, and the independent oversight of the use of those powers, ensures that any interference with privacy is necessary and proportionate. Decisions about the issuing of warrants to the ACT Integrity Commission authorising access to stored communications under the TIA Act would need to be made by an eligible Judge or nominated member of the Administrative Review Tribunal. Under section 116 of the Act, a warrant for access to a person’s stored communications may be issued where the issuing authority is satisfied that, among other things:

* information that would be likely to be obtained would be likely to assist in connection with the investigation of a serious contravention in which the person is involved, and
* having regard to a range of matters specified in the Act, including how much the privacy of any persons would be interfered with, the gravity of the conduct in question, the likely investigative value of the information, and the availability and likely effectiveness of alternative methods of investigation, that the warrant should be issued.

Authorised officers of the ACT Integrity Commission will only be permitted to authorise access to telecommunications data under sections 178, 179 or 180 of the TIA Act if they satisfied that access is reasonably necessary for an investigative purpose covered by those provisions, and are satisfied on reasonable grounds that any interference with privacy is justifiable and proportionate having regard to:

* the gravity of the conduct in relation to which the authorisation is sought
* the likely relevance and usefulness of the information, and
* the reason why the disclosure is proposed to be authorised.

As is the case with other criminal law-enforcement agencies that are authorised to exercise covert powers under Chapters 3 and 4 of the TIA Act, the Ombudsman would oversee the ACT Integrity Commission’s use of powers. Oversight by the Commonwealth Ombudsman would provide further assurance that the exercise of powers that limit the right to privacy are reasonable, necessary and proportionate.

***Conclusion***

This Declaration is made for the legitimate purpose of protecting 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.

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