

EXPLANATORY STATEMENT

Issued by the authority of the Attorney-General

Telecommunications (Interception and Access) Act 1979

Interception Capability Plan Determination 2024

Under Part 5-4 of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), all licensed telecommunications carriers, and those carriage service providers specifically nominated by the Attorney-General, are required to submit an annual interception capability plan (IC plan) to a Communications Access Coordinator. Subsection 195(2) of the TIA Act provides that the content of IC plans must include, *inter alia*, the carrier or nominated carriage service provider (C/NCSP)'s policies and strategies in relation to their interception responsibilities, the locations of interception points on their networks and a list of their employees with responsibility for interception matters.

Paragraph 195(4) of the TIA Act allows the Attorney-General to determine additional matters that must be set out in the IC plans of C/NCSPs that are specifically notified of the additional requirements. On 14 February 2018, the then Attorney-General made the *Interception Capability Plan Determination 2018 (No. 1)* (the previous Determination).

On 25 October 2024, amendments to the TIA Act took effect, substituting references to 'the Communications Access Co-ordinator' with 'a Communications Access Coordinator'. The *Interception Capability Plan Determination 2024* (the Determination) reflects this updated terminology in the TIA Act.

The Determination also applies the definition of 'Nominated carriage service provider' from the TIA Act, rather than re-stating the definition in slightly different terms (which was the approach taken in the 2018 Determination). This application of the definition in the TIA Act is intended to streamline the drafting of the instrument and to ensure consistency with the principal legislation.

Apart from these two minor changes, the Determination is made in terms identical to the previous 2018 Determination.

The Determination provides that if a C/NCSP has been notified in writing by a Communications Access Coordinator that C/NCSP must include in its IC plan a description of the arrangements that the C/NCSP will put in place, under the control of persons holding appropriate national security clearances, to provide interception capabilities within Australia. The notified C/NCSPs will also be required to protect information relating to interception and provide other reasonably necessary assistance relating to interception to national security and law enforcement agencies.

A number of C/NCSPs have been notified by the CAC that they must comply with the Determination, based on an assessment that these providers may choose to locate their interception capabilities offshore or place their interception capabilities under the control of non-Australian employees.

In accordance with section 195(5) of the TIA Act, the Attorney-General's Department consulted the Australian Communications and Media Authority on behalf of the Attorney-General before making this Determination.

The Determination is a legislative instrument for the purposes of the *Legislation Act 2003*.

Statement of Compatibility with Human Rights

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

Interception Capability Plan Determination 2024

This Determination 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 Determination

Under Part 5-4 of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), all licensed telecommunications carriers, and those carriage service providers specifically nominated by the Attorney-General, are required to submit an annual interception capability plan (IC plan) to a Communications Access Coordinator. Subsection 195(2) of the TIA Act provides that the content of IC plans must include, *inter alia*, the carrier or nominated carriage service provider (C/NCSP)'s policies and strategies in relation to their interception responsibilities, the locations of interception points on their networks and a list of their employees with responsibility for interception matters.

The *Interception Capability Plan Determination 2024* (the Determination) is made under section 195(4) of the TIA Act and sets out additional matters that must be included in an IC plan. The Determination is a legislative instrument for the purposes of the *Legislation Act 2003*.

The Determination provides that if a C/NCSP has been notified in writing by a Communications Access Coordinator, the C/NCSP must include in its IC plan a description of the arrangements that the C/NCSP will put in place to maintain their interception capability within Australia and under the control of persons holding appropriate national security clearances. The notified C/NCSPs must also protect information relating to interception and provide other reasonably necessary assistance relating to interception to national security and law enforcement agencies.

The Determination has been made in terms identical to the *Interception Capability Plan Determination 2018 (No. 1)*, aside from changing references to 'the Communications Access Co-ordinator' to 'a Communications Access Coordinator' and applying the definition of 'Nominated carriage service provider' from the TIA Act rather than re-stating the definition.

Human rights implications

The Determination engages the right to protection against arbitrary and unlawful interferences with privacy under article 17 of the *International Covenant on Civil and Political Rights* (ICCPR).

Article 17 - privacy

Article 17 of the ICCPR provides that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honour or reputation, and that everyone has the right to the protection of the law against such interference or attacks.

The use of the term 'arbitrary' 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. The United Nations Human Rights Committee has interpreted

‘reasonableness’ to imply that any limitation must be proportionate and necessary in the circumstances.

This instrument will require the provision of information, which will permit the oversight of capabilities required under existing legislation that limit the right to privacy under Article 17.

The right to privacy under the ICCPR can be limited as it is not an absolute right. The right can be limited if the limitation is not incompatible with the right itself and the limitation is authorised by law, is for a legitimate objective and is reasonable, necessary and proportionate to that objective. Interferences with privacy may be permissible where they are authorised by law and not arbitrary. In order for an interference with the right to privacy not to be arbitrary, the interference must be for a reason consistent with the provisions, aims and objectives of the ICCPR and be reasonable under the circumstances.

Interception of telecommunications may only occur subject to a warrant issued by an issuing authority, namely an eligible judge or a nominated member of the Administrative Review Tribunal. Before an issuing authority may issue a warrant they must be satisfied that interception is appropriate in the circumstances. In coming to this conclusion the issuing authority must consider several factors, including the privacy impacts of the interception, the gravity of the offence, the likely usefulness of interception information to the relevant investigation and the extent to which other methods of investigating the offence have been used or are available. To ensure the integrity of this regime, access to, and use of, interception material, stored communications and telecommunications data is subject to checks and balances as provided by the TIA Act. These measures ensure that an individual’s privacy is not unduly burdened. The instrument will require the provision of information relating to interception capabilities, which exist to serve the legitimate objective of the investigation and prosecution of serious crime and corruption and is reasonable, necessary and proportionate to achieving this end.

Conclusion

The instrument is compatible with human rights because it advances the protection of human rights, and to the extent that it limits human rights, those limitations are authorised by law, reasonable, necessary and proportionate.