EXPLANATORY STATEMENT

Issued by the Minister for Home Affairs

Telecommunications (Interception and Access) Act 1979

Telecommunications (Interception and Access) Amendment (International Production Orders) Regulations 2022

The *Telecommunications (Interception and Access) Act 1979* (the TIA Act) protects the privacy of, and regulates access to, the content of telecommunications and telecommunications data. It creates a legal framework for law enforcement and intelligence agencies to access information held by communications providers for the investigation of criminal offences and other activities that threaten safety and security. The TIA Act prohibits the interception of communications and access to stored communications, except in specified circumstances.

Schedule 1 to the TIA Act establishes an International Production Order (IPO) framework that enables Australian law enforcement and national security agencies to obtain independently-authorised orders for content or data that are directed to communications service providers in foreign countries with which Australia has a designated international agreement. Clause 3 of Schedule 1 to the Act provides that for a bilateral agreement to be a *designated international agreement* under the Act, there must be an agreement between Australia and a foreign country, the text of the agreement must be set out in the regulations and the agreement must have entered into force for Australia and the foreign country.

Section 300 of the TIA Act provides that the Governor-General may make regulations, not inconsistent with the Act, prescribing matters required or permitted by the Act to be prescribed, or necessary or convenient to be prescribed for carrying out or giving effect to the Act.

The *Telecommunications (Interception and Access) Amendment (International Production Orders) Regulations 2022* (the Regulations) amend the *Telecommunications (Interception and Access) Regulations 2017* to give effect in Australian domestic law to the *Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* (AUS-US CLOUD Act Agreement). The AUS-US CLOUD Act Agreement was signed by the Governments of Australia and the United States in Washington D.C. on 15 December 2021. Once the AUS-US CLOUD Act Agreement has been set out in regulations and has entered into force, it will become a *designated international agreement* for the purposes of the IPO regime in Schedule 1 to the TIA Act.

Communications platforms and services based overseas are often used to commit a range of serious crimes, such as terrorism, child sexual abuse, and cybercrime. This means that

electronic data relating to serious crimes, once traditionally available in Australia, is now held in foreign jurisdictions and subject to foreign laws.

International crime cooperation continues to be the key mechanism that Australian agencies use to obtain electronic data from foreign jurisdictions. However, current processes for obtaining electronic data held by service providers in other countries can be challenging, particularly in light of the increasing demand for electronic data by law enforcement investigations worldwide. Not being able to access this information in a timely manner significantly undermines efforts by Australian law enforcement and national security agencies. This can jeopardise criminal justice outcomes.

The AUS-US CLOUD Act Agreement will streamline the process for obtaining electronic data in Australia and the United States by establishing a clear framework for direct cooperation between government agencies and communications service providers in both countries. The AUS-US CLOUD Act Agreement ensures Australian and US law enforcement agencies have timely access to electronic data to prevent, detect, investigate and prosecute a covered offence. A covered offence is defined in the Agreement to mean conduct that, under the domestic law of the issuing party, constitutes a serious crime (punishable by at least three years' imprisonment or life). This is reflected in the definition of serious category 1 and 2 offences in Schedule 1 to the TIA Act.

The AUS-US CLOUD Act Agreement contains a number of important safeguards and human rights protections. For example, Article 9(4) of the Agreement allows parties to declare essential interests. The text of the Agreement and the side letters of understanding in relation to the death penalty will require the US to obtain Australia's permission to use Australian-sourced data obtained under the AUS-US CLOUD Act Agreement as evidence in the prosecution's case for an offence in which the death penalty is sought. Australia will retain the discretion to refuse permission, or to grant permission subject to such conditions as Australia considers necessary. This reflects Australia's policy position on the death penalty and domestic legal requirements.

Consultation was not undertaken outside of the Australian Government on the text of the AUS-US CLOUD Act Agreement. However, during negotiations State and Territory Government agencies were consulted on relevant features of the AUS-US CLOUD Act Agreement, and relevant industry stakeholders were consulted on matters relevant to their role in operationalising the AUS-US CLOUD Act Agreement.

In accordance with the treaty process, the text of the AUS-US CLOUD Act Agreement will be subject to parliamentary scrutiny, including consideration by the Joint Standing Committee on Treaties, and published on the Australian Treaties Library on the AustLII website. The Australian Government will undertake further consultation across government and industry now that the AUS-US CLOUD Act Agreement is publicly available.

Consultation was not undertaken outside of the Australian Government for these Regulations, as it functions only to give effect to the Agreement. The Regulations do not have a direct, or substantial indirect effect on business, nor does it restrict competition.

The TIA Act specifies two conditions that need to be satisfied before the power to make the Regulations can be exercised.

First, subclause 3(1A) of Schedule 1 to the TIA Act applies because the AUS-US CLOUD Act Agreement deals with the issue of orders by a competent authority of the US. Subclause 3(1A) provides the text of the agreement must not be set out in regulations unless a statutory requirements certificate (issued by the Attorney-General) is in force under clause 3B in relation to the US and the agreement. This condition was satisfied prior to the Regulations being made as the Attorney-General issued a statutory requirements certificate that is in force under clause 3B of Schedule 1 to the TIA Act.

Second, subclause 3(2) of Schedule 1 to the TIA Act applies because one or more offences against the law of the US are death penalty offences. Subclause 3(2) provides the text of the agreement must not be set out in regulations unless the Minister has received a written assurance from the US government, relating to the use or non-use of Australian-sourced information obtained by virtue of the agreement, in connection with any proceeding by way of a prosecution for a death penalty offence in the US. The Minister received this written assurance from the US Government by way of the signed AUS-US CLOUD Act Agreement (Article 9(4)) together with the exchange of letters of understanding in relation to the death penalty offences on 15 December 2021.

The Regulations commence on the day they take effect under subclause 3A(3) of Schedule 1 to the TIA Act.

After the Parliamentary review processes have been finalised in Australia and the Congressional review processes finalised in the US, Australia and the US will exchange diplomatic notes confirming each country is ready for entry into force. The Agreement will then enter into force and become operational on the date the exchange of diplomatic notes is completed.

A Statement of Compatibility with Human Rights (the Statement) has been completed in accordance with the *Human Rights (Parliamentary Scrutiny) Act 2011*. The overall assessment is that the Regulations are compatible with human rights. A copy of the Statement is at **Attachment A**.

Details of the Regulations are set out in **Attachment B**.

The Office of Best Practice Regulation (OBPR) has been consulted in relation to the amendments and has advised that a Regulation Impact Statement is not required. The OBPR reference is 25361.

The Regulations are a legislative instrument for the purposes of the *Legislative Instruments Act 2003*.

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) Amendment (International Production Orders) Regulations 2022

These Regulations are 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 Regulations

Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) establishes a framework that enables Australian law enforcement and national security agencies to obtain independently-authorised orders for data that are directed to communications service providers in foreign countries with which Australia has a designated international agreement. International Production Orders (IPOs) will be a key aspect in enabling international crime cooperation in a digitally connected world where key evidence of serious criminality is often distributed across multiple jurisdictions.

The *Telecommunications (Interception and Access) Amendment (International Production Orders) Regulations 2022* (the Regulations) amend *the Telecommunications (Interception and Access) Regulations 2017* to give effect in Australian domestic law to the *Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* (AUS-US CLOUD Act Agreement). The AUS-US CLOUD Act Agreement was signed by the Governments of Australia and the United States in Washington D.C. on 15 December 2021. The AUS-US CLOUD Act Agreement will become a *designated international agreement* for the purposes of the IPO regime in Schedule 1 to the TIA Act when it has both been set out in the regulations and entered into force.

Communications platforms and services based overseas are often used to commit a range of serious crimes, such as terrorism, child sexual abuse, and cybercrime. This means that electronic data relating to serious crimes, once traditionally available in Australia, is now held in foreign jurisdictions and subject to foreign laws.

International crime cooperation continues to be the key mechanism that Australian agencies use to obtain electronic data from foreign jurisdictions. However, current processes for obtaining electronic data held by service providers in other countries can be challenging, particularly in light of the increasing demand for electronic data by law enforcement investigations worldwide. Not being able to access this information in a timely manner

significantly undermines efforts by Australian law enforcement and national security agencies. This can jeopardise criminal justice outcomes.

The AUS-US CLOUD Act Agreement will streamline the process for obtaining electronic data in Australia and the United States by establishing a clear framework for direct cooperation between government agencies and communications service providers in both countries. The AUS-US CLOUD Act Agreement ensures Australian and US law enforcement agencies have timely access to electronic data to prevent, detect, investigate and prosecute a covered offence. A covered offence is defined in the Agreement to mean conduct that, under the domestic law of the issuing country, constitutes a serious crime (punishable by at least three years' imprisonment or life). This is reflected in the definition of serious category 1 and 2 offences in Schedule 1 to the TIA Act.

Human Rights Implications

The Regulations engage the following human rights under the *International Covenant on Civil and Political Rights* (ICCPR):

- protection against arbitrary or unlawful interference with privacy in Article 17 of the ICCPR, and
- the right to freedom of expression in Article 19 of the ICCPR.

Protection against arbitrary or unlawful interference with privacy in Article 17 of the ICCPR

The Regulations engage the protection against arbitrary or unlawful interference with privacy in Article 17 of the ICCPR. Article 17 prohibits unlawful or arbitrary interferences with a person's privacy. Collecting, using, storing, disclosing or publishing personal information amounts to an interference with privacy. In order for the interference with privacy not to be 'arbitrary', 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. Reasonableness, in this context, incorporates notions of proportionality, appropriateness and necessity.

The Regulations give effect in Australian domestic law to the AUS-US CLOUD Act Agreement. The purpose of the Agreement is to provide an efficient, effective, and privacy-protective means for Australia and the US to obtain electronic data for the purposes of prevention, detection, investigation, and prosecution of serious crime.

Where a designated international agreement is in place under the IPO regime, the AUS-US CLOUD Act Agreement enables Australian communications service providers to facilitate the US government's access to private communications data, where an appropriate order is in place. This will engage and limit the protection against arbitrary and unlawful interference with privacy in Article 17 of the ICCPR.

While the measures will limit the right to privacy in Article 17 of the ICCPR, the limitation is reasonable, necessary and proportionate in achieving the legitimate objective of facilitating the prevention, detection, investigation and prosecution of serious crime in an increasingly digitally connected world where key evidence of serious criminality is often distributed across multiple jurisdictions. Article 3(3) of the AUS-US CLOUD Act Agreement notes that each party recognises that the domestic legal framework of the other party, including the implementation of that framework, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities subject to the Agreement. Subclause 3B(2) of Schedule 1 to the TIA Act enables the Attorney-General, after consulting the Minister for Home Affairs and the Minister for Foreign Affairs, to issue a statutory requirements certificate in relation to:

- a foreign country that is party to the agreement; and
- the agreement.

Paragraph 3(1A)(b) states that an agreement cannot be set out in regulations unless a statutory requirements certificate is in force under clause 3B. Furthermore, subparagraphs 3B(4)(c)(i) and 3B(4)(c)(i) of Schedule 1 to the TIA Act require that the Attorney-General must not issue a statutory requirements certificate unless the foreign country has demonstrated respect for the rule of law, and has demonstrated respect for human rights relevant to cross-border access to data in its domestic laws and policies.

This process provides a mechanism for the Australian Parliament and public to be assured that the data of Australians will not be targeted by incoming orders, that Australian-sourced data will be appropriately collected and protected, and that the agreement is with a trusted foreign country that acts in a manner consistent with the rule of law and internationally recognised human rights. The Attorney-General has issued this statutory requirements certificate, confirming the US meets these requirements.

Requirements and limitations on orders

The AUS-US CLOUD Act Agreement contains a number of requirements and limitations on orders that may be issued under the Agreement that help protect against arbitrary and unlawful interference with privacy. For example:

- orders must be for the purposes of obtaining information relating to the prevention, detection, investigation or prosecution of serious crime (Article 4(1))
- orders must be subject to independent review or oversight (Article 5(2))
- orders must target a specific account, and must not intentionally target Australian citizens, permanent residents, corporations, government entities of, or persons located in Australia (Article 4(5) and (3)), and
- orders for interception must be for a fixed, limited duration and shall not last longer than is reasonably necessary (Article 5(3)).

Orders for data that do not meet these requirements must be pursued through alternative mechanisms, such as mutual legal assistance.

Targeting restrictions

The AUS-US CLOUD Act Agreement is focussed on allowing Australia and the US to gather evidence in relation to crimes committed by their own citizens, located in their own jurisdiction. The Agreement includes specific prohibitions on the targeting of each other's citizens and people located in the other's jurisdiction. Articles 4(3) and 4(4) of the Agreement will ensure that US orders cannot intentionally target Australian persons, including citizens, permanent residents, corporations, non-incorporated associations like charities, government entities and persons physically located in Australia. Both Australia and the United States will adopt procedures to minimise the acquisition, retention, and dissemination of information concerning each other's citizens or permanent residents where their communications were incidentally obtained.

Privacy and data protection safeguards

Article 3(4) of the AUS-US CLOUD Act Agreement requires each party to ensure personal data received under the Agreement is protected in accordance with its domestic legal framework, and sets out several fundamental protections for privacy provided under that legal framework (subject to reasonable restrictions). Articles 7 and 9 also provide a range of safeguards and requirements related to the collection, handling, use and disclosure of data. By implementing the AUS-US CLOUD Act Agreement into domestic law, the Regulations also introduce these safeguards into the IPO regime.

Proportionality

Article 4(1) of the AUS-US CLOUD Act Agreement requires that orders subject to this Agreement shall be for the purpose of obtaining information relating to a covered offence, defined in Article 1 as conduct that under the domestic law of the issuing party constitutes a serious crime. Clause 2 of Schedule 1 to the TIA Act defines serious crime as either:

- serious category 1 offence
    - punishable by imprisonment for three years or more; or
    - punishable by imprisonment for life
- serious category 2 offence
    - punishable by imprisonment for 7 years or more; or
    - punishable by imprisonment life

In deciding whether to issue an IPO, the decision maker must have regard to several matters including, relevantly, how much the privacy of any person or persons would be likely to be interfered with. For IPOs relating to control orders, the decision maker must consider whether intercepting communications would be the method that is likely to have the least interference with any person's privacy. These safeguards help ensure that the measures are the least rights restrictive option when obtaining the necessary information.

Paragraph 30(2)(g) of Schedule 1 to the TIA Act requires that in issuing an IPO for interception, the issuing authority must agree that the order will assist in the investigation of a serious category 2 offence. For IPOs related to stored communications and telecommunications data, issuing authorities must agree the order will assist in the investigation of a serious category 1 offence. These safeguards ensure that the AUS-US CLOUD Act Agreement be used solely for the purpose of combating serious crime, with strict thresholds on the issuing of interception orders that are consistent with the Australian domestic framework. The limitation on the right to privacy is proportionate, as IPOs can only be issued in relation to serious criminal offences and cannot be targeted at certain persons.

The Regulations do not constitute an arbitrary or unlawful interference with the right to privacy. The limitation on the protection against arbitrary or unlawful interference with privacy is reasonable, necessary and proportionate to achieving a legitimate objective.

The right to freedom of expression in Article 19 of the ICCPR

Article 19(2) of the ICCPR provides everyone shall have the right to freedom of expression, including the right 'to seek, receive and impart information and ideas of all kinds and regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice'. Furthermore, Article 19(3) of the ICCPR provides that the exercise of the rights provided for in Article 19(2) carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary for the protection of national security or of public order, or of public health or morals.

The AUS-US CLOUD Act Agreement and Australia's IPO framework may engage the right to freedom of expression by indirectly making some people more reluctant to use communications services. It is plausible that a person may minimise their use of communication services if they know government agencies can seek prescribed communications providers to provide communications carried through these services. By implementing the AUS-US CLOUD Act Agreement into domestic legislation, the Regulations may engage this right.

To the extent that a person in Australia may minimise the use of a prescribed communications provider in the United States out of concern that Australian law enforcement authorities may seek an order for their data held by that communications provider, Article 19(3) may be engaged. However, any limitation is reasonable, necessary and proportionate in achieving the legitimate objective of protecting national security or public order. As noted above, a number of safeguards apply when seeking IPOs, and IPOs can only be sought in relation to certain serious crimes. Further, designated authorities are required to take into account a number of matters before complying with an order and Article 4(2) of the AUS-US CLOUD Act Agreement prohibits orders subject to the Agreement from being used to infringe freedom of speech or for disadvantaging persons based on their race, sex, sexual orientation, religion, ethnic origin, or political opinions.

To the extent that implementing the AUS-US CLOUD Act Agreement into domestic legislation does limit the right to freedom of expression, such a limitation is reasonable, necessary and proportionate for the protection of national security or of public order.

Conclusion

The Regulations are compatible with human rights as, to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate.

The Hon Karen Andrews MP

Minister for Home Affairs

ATTACHMENT B

Details of the *Telecommunications (Interception and Access) Amendment (International Production Orders) Regulations 2022*

Section 1 – Name

This section provides that the name of the instrument is the *Telecommunications (Interception and Access) Amendment (International Production Orders) Regulations 2022* (the Regulations).

Section 2 – Commencement

This section provides that the commencement date for this instrument is the day this instrument takes effect under subclause 3A(3) of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979* (the Act).

Subclause 3A(2) of Schedule 1 to the Act provides that either House of Parliament may, following a motion upon notice, pass a resolution disallowing the regulations. For the notice to be effective, the notice must have been given in that House of Parliament within 15 sitting days of that House after a copy of the regulations was tabled in that House and the resolution must be passed within 15 sitting days of that House after the giving of that notice. This ensures that regulations setting out the text of an agreement or the text of an amendment to a designated international agreement will be subject to parliamentary scrutiny and potential disallowance.

Pursuant to subclause 3A(3), if neither House passes a resolution to disallow the regulations, the regulations will take effect on the day immediately after the last day upon which a disallowance resolution could have been passed. This makes clear that regulations made for the purposes of clause 3 are subject to parliamentary scrutiny and cannot commence until after a period of 30 sitting days in each House has occurred. The commencement provision in section 2 of the Regulations is drafted to align with subclause 3A(3) of Schedule 1 to the Act.

Subclause 3A(4) provides for circumstances where the regulations will be deemed to have been disallowed. In these circumstances, subclause 3A(3) does not apply, meaning the regulations would not take effect.

Section 3 – Authority

This section provides that the instrument is made under the Act.

Section 4 – Schedules

This section provides for how the amendments in the Regulations operate.

Schedule 1 – Amendments

Telecommunications (Interception and Access) Regulations 2017

Item [1] – After Part 3

This item inserts new Part 3A – International production orders, and new section 26A to the *Telecommunications (Interception and Access) Regulations 2017*.

New section 26A provides that for the purposes of paragraph 3(1)(b) of Schedule 1 to the Act, a copy of the English text of the Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime (the AUS-US CLOUD Act Agreement), is set out in Schedule 2 to the *Telecommunications (Interception and Access) Regulations 2017.*

New Schedule 2 to the *Telecommunications (Interception and Access) Regulations 2017* is added by item 2.

Item [2] – At the end of the instrument

This item adds a Schedule 2 to the *Telecommunications (Interception and Access) Regulations 2017* which sets out the English text of the AUS-US CLOUD Act Agreement.

The note following the heading to Schedule 2 directs the reader to section 26A, inserted by item [1] above.

The AUS-US CLOUD Act Agreement was signed in Washington D.C. on 15 December 2021. Once the AUS-US CLOUD Act Agreement has been set out in regulations and once it has entered into force (after both countries' Parliamentary or Congressional review processes have been finalised and diplomatic notes have been exchanged), it will become a *designated international agreement* for the purposes of the International Production Order regime in Schedule 1 to the Act.