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

I, General the Honourable David Hurley AC DSC (Retd), Governor-General of the Commonwealth of Australia, acting with the advice of the Federal Executive Council, make the following regulations.

Dated 03 February 2022

David Hurley
Governor-General

By His Excellency's Command

Karen Andrews
Minister for Home Affairs

Contents

1 Name

This instrument is the *Telecommunications (Interception and Access) Amendment (International Production Orders) Regulations 2022*.

2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. The whole of this instrument	The day this instrument takes effect under subclause 3A(3) of Schedule 1 to the *Telecommunications (Interception and Access) Act 1979*.	30 November 2022

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under the *Telecommunications (Interception and Access) Act 1979*.

4 Schedules

Each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

Schedule 1—Amendments

Telecommunications (Interception and Access) Regulations 2017

1 After Part 3

Insert:

Part 3A—International production orders

26A Designated international agreement—Australia-US CLOUD Act Agreement

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 is set out in Schedule 2 to this instrument.

2 At the end of the instrument

Add:

Schedule 2—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

Note: See section 26A.

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

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 Government of Australia and the Government of the United States of America (hereinafter the "Parties");

Prompted by the Parties' mutual interest in enhancing their cooperation for the purpose of protecting public safety and combating serious crime, including terrorism;

Recognizing that timely access to electronic data for authorized law enforcement purposes is an essential component in this effort;

Emphasizing the importance of, and common commitment to, respecting the protection of privacy, human rights and civil liberties, including freedom of speech, and the rule of law;

Noting the harms of data localization requirements to a free, open, and secure Internet, and endeavoring to avoid such requirements; and

Recognizing that both Parties' respective legal frameworks for accessing electronic data incorporate appropriate and substantial safeguards for protecting privacy and civil liberties, including, as applicable, the requirements of probable cause or reasonable grounds to suspect, and independent review or oversight, when accessing the content of communications;

Have agreed as follows:

Article 1: Definitions

For the purposes of this Agreement:

1. **Account** means the means, such as an account, telephone number, or addressing information, through which a user gains personalized access to a Computer System or telecommunications system.
2. **Australian Person** means (i) a citizen of Australia; (ii) a permanent resident of Australia; (iii) an unincorporated association with a substantial number of members of which fall into subparagraphs (i) or (ii); or (iv) a corporation that is incorporated in Australia.
3. **Computer System** has the meaning set forth in Chapter 1 Article 1a of the Council of Europe Convention on Cybercrime: any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.
4. **Covered Data** means the following types of data when possessed or controlled by a private entity acting in its capacity as a Covered Provider: content of an electronic or wire communication; computer data stored or processed for a user; traffic data or metadata pertaining to an electronic or wire communication or the storage or processing of computer data for a user; and Subscriber Information when sought pursuant to an Order that also seeks any of the other types of data referenced in this definition.
5. **Covered Offense** means conduct that, under the law of the Issuing Party, constitutes a Serious Crime, including terrorist activity.
6. **Covered Person** means a person who, upon application of the procedures required by Article 7.1, is reasonably believed not to be a Receiving-Party Person at the time the Agreement is invoked for an Order pursuant to Article 5.
7. **Covered Provider** means any private entity to the extent that it: (i) provides to the public the ability to communicate, or to process or store computer data, by means of a Computer System or a telecommunications system; or (ii) processes or stores Covered Data on behalf of an entity defined in subparagraph (i).
8. **Designated Authority** means for Australia, the governmental entity designated by the Minister for Home Affairs, and for the United States, the Attorney General or a person designated by the Attorney General.
9. **Issuing Party** means the Party, including political subdivisions thereof, that issues the relevant Legal Process and, where applicable, invokes this Agreement. Where the United States is the Issuing Party, this includes Legal Process issued by federal, state, local, or territorial authorities within the United States. Where Australia is the Issuing Party, this includes Legal Process issued by Commonwealth, state or territory authorities within Australia.
10. **Legal Process** means Orders subject to this Agreement as well as process related to the preservation of Covered Data or to the preservation, disclosure, production or authentication of Subscriber Information.
11. **Order** means a legal instrument issued under the domestic law of the Issuing Party requiring the disclosure or production of Covered Data (including any

requirement to authenticate such data) by a Covered Provider, including for stored or live communications.

12. **Personal Data** means information relating to an identified or identifiable individual.
13. **Receiving-Party Person** means (i) any governmental entity, including a federal entity or an entity of a political subdivision thereof, of the Receiving Party; (ii) a citizen or national of the Receiving Party; (iii) a person lawfully admitted for permanent residence in the Receiving Party; (iv) an unincorporated association a substantial number of members of which fall into subparagraphs (ii) or (iii); (v) a corporation that is incorporated in the Receiving Party; or (vi) a person located in the territory of the Receiving Party.
14. **Receiving Party** means the Party, including political subdivisions thereof, other than the Issuing Party.
15. **Serious Crime** means an offense punishable by a maximum term of imprisonment of at least three years.
16. **Subscriber Information** means information that identifies a subscriber or customer of a Covered Provider, including name, address, length and type of service, subscriber number or identity (including assigned network address and device identifiers) telephone connection records, records of session times and durations, and means of payment.
17. **U.S. Person** means: (i) a citizen or national of the United States; (ii) a person lawfully admitted for permanent residence in the United States; (iii) an unincorporated association a substantial number of members of which fall into subparagraphs (i) or (ii); or (iv) a corporation that is incorporated in the United States.

Article 2: Purpose of the Agreement

The purpose of this Agreement is to advance public safety and security, and to protect privacy rights, civil liberties, and an open Internet, by resolving potential conflicts of legal obligations when communications service providers are served with Legal Process from one Party for the production or preservation of electronic data, where those providers may also be subject to the laws of the other Party. To that end, this Agreement provides an efficient, effective, and privacy-protective means for each Party to obtain electronic data for the purposes of prevention, detection, investigation, and prosecution of serious crime in a manner consistent with its domestic legal framework and the domestic legal framework of the other Party, and use that data subject to appropriate targeting and use restrictions and privacy protections, and consistent with each Party's international human rights and other international law obligations.

Article 3: Domestic Law and Effect of the Agreement

1. Each Party undertakes to ensure that its domestic laws relating to the preservation, authentication, disclosure, and production of electronic data permit Covered Providers to comply with Legal Process. Each Party shall advise the other of any material changes in its domestic laws that would substantially frustrate or impair the operation of this Agreement.

2. The provisions of this Agreement referring to an Order subject to this Agreement shall apply to an Order as to which the Issuing Party invokes this Agreement and notifies the relevant Covered Provider of that invocation. Any legal effect of Legal Process derives solely from the law of the Issuing Party. Covered Providers retain otherwise existing rights to raise applicable legal objections to Legal Process.

3. Each Party in executing this Agreement recognizes 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 this Agreement.

4. Personal Data received pursuant to Legal Process from a Covered Provider shall be protected in accordance with the domestic legal framework of the Issuing Party. Protections for privacy include, subject to reasonable restrictions under each Party's domestic legal framework:

    a. limiting the use and disclosure of Personal Data to purposes not incompatible with the purpose for which it was obtained;

    b. limiting retention of Personal Data for only as long as necessary and appropriate;

    c. safeguards to protect against loss or accidental or unauthorized access, disclosure, alteration, or destruction of Personal Data;

    d. a framework for individuals to seek and obtain access to Personal Data concerning them, and to seek correction of Personal Data that is inaccurate, when appropriate; and

    e. a framework to respond to complaints from individuals.

5. Each Party shall advise the other of any material changes in its domestic law that significantly affect the protections for data received pursuant to Legal Process and shall consult regarding any issues arising under this paragraph pursuant to Article 5 or Article 11.

6. This Agreement is intended to facilitate the ability of the Parties to obtain certain electronic data. The provisions of this Agreement shall not give rise to a right or remedy on the part of any private person, including to obtain, suppress or exclude any evidence, or to impede the execution of Legal Process. Each Party

shall ensure that the provisions of this Agreement are implemented consistent with its fundamental principles governing the relationship between its central government and constituent states or other similar territorial entities.

Article 4: Targeting Restrictions

1. Orders subject to this Agreement shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of a Covered Offense.
2. Orders subject to this Agreement shall not be used to infringe freedom of speech or for disadvantaging persons based on their race, sex, sexual orientation, religion, ethnic origin or political opinions.
3. Orders subject to this Agreement shall not intentionally target a Receiving-Party Person, and each Party shall adopt targeting procedures designed to implement this requirement as described in Article 7.1.
4. Orders subject to this Agreement shall not target a Covered Person if the purpose is to obtain information concerning a Receiving-Party Person.
5. Orders subject to this Agreement shall be targeted at specific Accounts, and shall identify as the object of the Order a specific person, account, address, or personal device, or other specific identifier.

Article 5: Issuance and Transmission of Orders

1. Orders subject to this Agreement shall be issued in compliance with the domestic law of the Issuing Party, and shall be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation.
2. Orders subject to this Agreement shall be subject to review or oversight under the domestic law of the Issuing Party by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the Order.
3. Orders subject to this Agreement for the interception of wire or electronic communications, and any extensions thereof, shall be for a fixed, limited duration; shall not last longer than is reasonably necessary to accomplish the approved purposes of the Order; and shall be issued only if the same information could not reasonably be obtained by another less intrusive method.
4. The Issuing Party shall not issue an Order subject to this Agreement at the request of or to obtain information to provide to the Receiving Party or a third-party government.

5. The Issuing Party may issue Orders subject to this Agreement directly to a Covered Provider. Orders subject to this Agreement shall be transmitted by the Issuing Party's Designated Authority. The Designated Authorities of the Parties may mutually decide that the functions each carries out under Articles 5.5 through and inclusive of 5.9, 6.1, and 6.2 may be performed by additional authorities of their governments in whole or in part. The Designated Authorities of the Parties may, by mutual decision, prescribe rules and conditions for any such authorities.

6. Prior to transmission, the Issuing Party's Designated Authority shall review the Orders for compliance with this Agreement.

7. Each Order subject to this Agreement must include a written certification by the Issuing Party's Designated Authority that the Order is lawful and complies with the Agreement, including the Issuing Party's substantive standards for Orders subject to this Agreement.

8. The Issuing Party's Designated Authority shall notify the Covered Provider that it invokes this Agreement with respect to an Order.

9. The Issuing Party shall notify the Covered Provider of a point of contact at the Issuing Party's Designated Authority who can provide information on legal or practical issues relating to the Order.

10. In cases where an Order subject to this Agreement is issued for data in respect of an individual who is reasonably believed to be located outside the territory of and is not a national, citizen, or a lawful permanent resident of the Issuing Party, the Issuing Party's Designated Authority shall notify the appropriate authorities in the third country where the person is located, except in cases where the Issuing Party considers that it would be detrimental to operational or national security, or impede the conduct of an investigation, or imperil human rights.

11. The Parties agree that a Covered Provider that receives an Order subject to this Agreement may raise specific objections when it has reasonable belief that the Agreement may not properly be invoked with regard to the Order. Such objections should generally be raised in the first instance to the Issuing Party's Designated Authority and in a reasonable time after receiving an Order. Upon receipt of objections to the Order from a Covered Provider, the Issuing Party's Designated Authority shall respond to the objections. If the objections are not resolved, the Parties agree that the Covered Provider may raise the objections to the Receiving Party's Designated Authority. The Parties' Designated Authorities may confer in an effort to resolve any such objections and may meet periodically and as necessary to discuss and address any issues raised under this Agreement.

12. If the Receiving Party's Designated Authority concludes that the Agreement may not properly be invoked with respect to any Order subject to this

Agreement, it shall notify the Issuing Party's Designated Authority and the relevant Covered Provider of that conclusion, and this Agreement shall not apply to that Order.

Article 6: Production of Information by Covered Providers

1. The Parties agree that any Covered Data produced by a Covered Provider in response to an Order subject to this Agreement should be produced directly to the Issuing Party's Designated Authority.
2. The Designated Authority of the Issuing Party may make arrangements with Covered Providers for the secure transmission of Orders subject to this Agreement and Covered Data produced in response to Orders subject to this Agreement, consistent with applicable law.
3. This Agreement does not in any way restrict or eliminate any obligation Covered Providers have to produce data pursuant to the law of the Issuing Party.
4. The Issuing Party's requirements as to the manner in which a Covered Provider responds to an Order may include that a Covered Provider complete forms that attest to the authenticity of records produced, or to the absence or non-existence of such records, and that the Order and any information or evidence furnished in response be kept confidential.

Article 7: Targeting and Minimization Procedures

1. Each Party shall adopt and implement appropriate targeting procedures, through which good-faith, reasonable efforts shall be employed to establish that any Account targeted by an Order subject to this Agreement is used or controlled by a Covered Person.
2. Australia and the United States shall adopt and implement appropriate procedures to minimize the acquisition, retention and dissemination of information concerning U.S. Persons and Australian Persons respectively acquired pursuant to an Order subject to this Agreement, consistent with the need of the Parties to acquire, retain, and disseminate Covered Data relating to the prevention, detection, investigation, or prosecution of a Covered Offense.
3. The minimization procedures for information acquired pursuant to an Order subject to this Agreement shall include rules requiring Parties to segregate, seal, or delete, and not disseminate material found not to be information that is, or is necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of a Covered Offense, or necessary to protect against a threat of death or serious bodily harm to any person.

4. The minimization procedures shall include rules requiring Parties to promptly review material collected pursuant to an Order subject to this Agreement and store any unreviewed communications on a secure system accessible only to those persons trained in applicable procedures.

5. The minimization procedures shall include a provision stating that Australia must not disseminate to the United States the content of a communication of a U.S. Person acquired pursuant to an Order subject to this Agreement, unless the communication may be disseminated pursuant to the minimization procedures and relates to significant harm, or the threat thereof, to the United States or U.S. Persons, including crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud.

6. Each Party shall develop those targeting and minimization procedures it is required by this Article to adopt in consultation with and subject to the approval of the other Party, and shall seek the approval of the other Party for any changes in those procedures.

Article 8: Preservation Process and Subscriber Information Process

1. The Issuing Party may issue and transmit Legal Process that solely seeks the preservation of Covered Data or the preservation, disclosure, production, or authentication of Subscriber Information directly to a Covered Provider. Such process must relate to the prevention, detection, investigation, or prosecution of crime and shall be issued in compliance with and subject to review or oversight as appropriate under the domestic law of the Issuing Party.

2. An Issuing Party and a Covered Provider may make arrangements for the secure transmission of the Legal Process referenced in paragraph 1 of this Article and Subscriber Information produced in response, consistent with applicable law.

3. The Issuing Party's requirements as to the manner in which a Covered Provider responds to Legal Process referenced in paragraph 1 of this Article may include that a Covered Provider complete forms that attest to the authenticity of the records produced, or to the absence or non-existence of such records, and that the Legal Process and any information or evidence furnished in response be kept confidential.

Article 9: Limitations on Use and Transfer

1. Data acquired by the Issuing Party pursuant to Legal Process shall be treated in accordance with the Issuing Party's domestic law, including its privacy and freedom of information laws.

2. The Issuing Party shall not transfer data received pursuant to an Order subject to this Agreement to a third-party government or international organization without

first obtaining the consent of the Receiving Party, except to the extent that such data has already been made public in accordance with the Issuing Party's domestic law.

3. The Issuing Party shall not be required to share any information produced pursuant to Legal Process with the Receiving Party or a third-party government.

4. Where an Issuing Party has received data pursuant to Legal Process from a Covered Provider, and:

    a. Australia has declared that its essential interests may be implicated by the introduction of such data as evidence in the prosecution's case in the United States for an offense for which the death penalty is sought; or

    b. the United States has declared that its essential interests may be implicated by the introduction of such data as evidence in the prosecution's case in Australia in a manner that raises freedom of speech concerns for the United States;

    prior to use of the data in a manner that is or could be contrary to those essential interests, the Issuing Party shall, via the Receiving Party's Designated Authority, obtain permission to do so. The Receiving Party may grant permission, subject to such conditions as it deems necessary, and if it does so, the Issuing Party may only introduce this data in compliance with those conditions. If the Receiving Party does not grant approval, the Issuing Party shall not use the data it has received pursuant to the Legal Process in that manner.

5. Use limitations additional to those specified in this Agreement may be imposed to the extent mutually agreed upon by the Parties.

Article 10 Compatibility and Non-Exclusivity

The Agreement is without prejudice to and shall not affect other legal authorities and mechanisms for the Issuing Party to obtain or preserve electronic data from the Receiving Party and from Covered Providers subject to the jurisdiction of the Receiving Party, including, but not limited to, legal instruments and practices under the domestic law of either Party as to which the Party does not invoke this Agreement; requests for mutual legal assistance; and emergency disclosures.

Article 11: Review of Implementation and Consultations

1. Within one year of this Agreement's entry into force, and periodically thereafter as mutually decided by the Parties, the Parties shall engage in a review of each Party's compliance with the terms of this Agreement, which may include a review of the issuance and transmission of Orders subject to this Agreement to

ensure that the purpose and provisions of this Agreement are being fulfilled, and a review of the Party's handling of data acquired pursuant to an Order subject to this Agreement to determine whether to modify procedures adopted under this Agreement.

2. The Parties may consult at other times as necessary or to resolve disputes concerning the implementation of this Agreement, and any such disputes shall not be referred to any court, tribunal, or third party.

3. Each Issuing Party's Designated Authority shall issue an annual report to the Receiving Party's Designated Authority reflecting aggregate data concerning its use of this Agreement to the extent consistent with operational or national security.

4. This Agreement does not in any way restrict or eliminate a Covered Provider's reporting of statistical information, consistent with applicable law, regarding Legal Process received by the Covered Provider.

Article 12: Costs

Each Party shall bear its own costs arising from the operation of this Agreement.

Article 13: Amendments

This Agreement may be amended by written agreement of the Parties at any time. Any such amendment shall enter into force on the date of the later note completing an exchange of diplomatic notes between the Parties indicating that each has taken the necessary steps to bring the amendment into force.

Article 14: Temporal Application

This Agreement shall apply to Legal Process issued by an Issuing Party on or after the Agreement's entry into force, regardless of whether the offense at issue was committed before or after this Agreement's entry into force.

Article 15: Entry into Force

This Agreement shall enter into force on the date of the later note completing an exchange of diplomatic notes between the Parties indicating that each has taken the steps necessary to bring the agreement into force.

Article 16: Expiry and Termination of the Agreement

1. This Agreement shall remain in force for a five year period. The Parties may agree in writing to extensions of the Agreement.
2. Separately from expiration under paragraph 1, this Agreement may be terminated by either Party by sending a written notification to the other Party through diplomatic channels. Termination shall become effective one month after the date of such notice.
3. In the event the Agreement expires or is terminated, the provisions of this Agreement shall continue to apply with respect to Orders subject to this Agreement already issued prior to the date on which the Agreement terminates or expires.
4. In the event the Agreement expires or is terminated, any data produced to the Issuing Party may continue to be used, and shall continue to be subject to the conditions and safeguards, including minimization procedures, set forth in this Agreement.

IN WITNESS WHEREOF, the undersigned, being duly authorized by their respective governments, have signed this Agreement.

Done at _____ this _____ day of _____, in duplicate, in the English language.

FOR THE GOVERNMENT OF AUSTRALIA:

FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA: