



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

DEC 22 2021

The Honorable Richard J. Durbin
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Pursuant to sections 2523(b) and (d) of Title 18 of the United States Code, the Department of Justice transmits the following documents to the Senate Judiciary Committee, the Senate Foreign Relations Committee, the House Judiciary Committee and the House Foreign Affairs Committee:

- Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), with side letters concerning the implementation and application of the Agreement;
- Certification by the Attorney General of his determination that the Agreement satisfies the requirements of section 2523(b); and
- Explanation of each consideration in determining that the Agreement satisfies the requirements of section 2523(b).

We hope this information is helpful. Please do not hesitate to contact this office if we can provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in blue ink that reads "Peter S. Hyun".

Peter S. Hyun
Acting Assistant Attorney General

Enclosures



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

DEC 22 2021

The Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Grassley:

Pursuant to sections 2523(b) and (d) of Title 18 of the United States Code, the Department of Justice transmits the following documents to the Senate Judiciary Committee, the Senate Foreign Relations Committee, the House Judiciary Committee and the House Foreign Affairs Committee:

- Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), with side letters concerning the implementation and application of the Agreement;
- Certification by the Attorney General of his determination that the Agreement satisfies the requirements of section 2523(b); and
- Explanation of each consideration in determining that the Agreement satisfies the requirements of section 2523(b).

We hope this information is helpful. Please do not hesitate to contact this office if we can provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in blue ink that reads "Peter S. Hyun".

Peter S. Hyun
Acting Assistant Attorney General

Enclosures



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

DEC 22 2021

The Honorable Robert Menendez
Chairman
Committee on Foreign Relations
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Pursuant to sections 2523(b) and (d) of Title 18 of the United States Code, the Department of Justice transmits the following documents to the Senate Judiciary Committee, the Senate Foreign Relations Committee, the House Judiciary Committee and the House Foreign Affairs Committee:

- Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), with side letters concerning the implementation and application of the Agreement;
- Certification by the Attorney General of his determination that the Agreement satisfies the requirements of section 2523(b); and
- Explanation of each consideration in determining that the Agreement satisfies the requirements of section 2523(b).

We hope this information is helpful. Please do not hesitate to contact this office if we can provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "Peter S. Hyun".

Peter S. Hyun
Acting Assistant Attorney General

Enclosures



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

DEC 22 2021

The Honorable James Risch
Ranking Member
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Senator Risch:

Pursuant to sections 2523(b) and (d) of Title 18 of the United States Code, the Department of Justice transmits the following documents to the Senate Judiciary Committee, the Senate Foreign Relations Committee, the House Judiciary Committee and the House Foreign Affairs Committee:

- Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), with side letters concerning the implementation and application of the Agreement;
- Certification by the Attorney General of his determination that the Agreement satisfies the requirements of section 2523(b); and
- Explanation of each consideration in determining that the Agreement satisfies the requirements of section 2523(b).

We hope this information is helpful. Please do not hesitate to contact this office if we can provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in blue ink that reads "Peter S. Hyun".

Peter S. Hyun
Acting Assistant Attorney General

Enclosures



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

DEC 22 2021

The Honorable Jerrold Nadler
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Pursuant to sections 2523(b) and (d) of Title 18 of the United States Code, the Department of Justice transmits the following documents to the Senate Judiciary Committee, the Senate Foreign Relations Committee, the House Judiciary Committee and the House Foreign Affairs Committee:

- Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), with side letters concerning the implementation and application of the Agreement;
- Certification by the Attorney General of his determination that the Agreement satisfies the requirements of section 2523(b); and
- Explanation of each consideration in determining that the Agreement satisfies the requirements of section 2523(b).

We hope this information is helpful. Please do not hesitate to contact this office if we can provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "Peter S. Hyun".

Peter S. Hyun
Acting Assistant Attorney General

Enclosures



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

DEC 22 2021

The Honorable Jim Jordan
Ranking Member
United States House of Representatives
Washington, D.C. 20515

Dear Representative Jordan:

Pursuant to sections 2523(b) and (d) of Title 18 of the United States Code, the Department of Justice transmits the following documents to the Senate Judiciary Committee, the Senate Foreign Relations Committee, the House Judiciary Committee and the House Foreign Affairs Committee:

- Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), with side letters concerning the implementation and application of the Agreement;
- Certification by the Attorney General of his determination that the Agreement satisfies the requirements of section 2523(b); and
- Explanation of each consideration in determining that the Agreement satisfies the requirements of section 2523(b).

We hope this information is helpful. Please do not hesitate to contact this office if we can provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in blue ink that reads "Peter S. Hyun".

Peter S. Hyun
Acting Assistant Attorney General

Enclosures



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

DEC 22 2021

The Honorable Gregory Meeks
Chairman
Committee on Foreign Affairs
United States House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Pursuant to sections 2523(b) and (d) of Title 18 of the United States Code, the Department of Justice transmits the following documents to the Senate Judiciary Committee, the Senate Foreign Relations Committee, the House Judiciary Committee and the House Foreign Affairs Committee:

- Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), with side letters concerning the implementation and application of the Agreement;
- Certification by the Attorney General of his determination that the Agreement satisfies the requirements of section 2523(b); and
- Explanation of each consideration in determining that the Agreement satisfies the requirements of section 2523(b).

We hope this information is helpful. Please do not hesitate to contact this office if we can provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "Peter Hyun", with a stylized flourish at the end.

Peter S. Hyun
Acting Assistant Attorney General

Enclosures



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

DEC 22 2021

The Honorable Michael McCaul
Ranking Member
Committee on Foreign Affairs
United States House of Representatives
Washington, D.C. 20515

Dear Representative McCaul:

Pursuant to sections 2523(b) and (d) of Title 18 of the United States Code, the Department of Justice transmits the following documents to the Senate Judiciary Committee, the Senate Foreign Relations Committee, the House Judiciary Committee and the House Foreign Affairs Committee:

- Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), with side letters concerning the implementation and application of the Agreement;
- Certification by the Attorney General of his determination that the Agreement satisfies the requirements of section 2523(b); and
- Explanation of each consideration in determining that the Agreement satisfies the requirements of section 2523(b).

We hope this information is helpful. Please do not hesitate to contact this office if we can provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "Peter S. Hyun".

Peter S. Hyun
Acting Assistant Attorney General

Enclosures

AGREEMENT
BETWEEN
THE GOVERNMENT OF THE UNITED STATES OF AMERICA
AND
THE GOVERNMENT OF AUSTRALIA
ON
ACCESS TO ELECTRONIC DATA FOR THE PURPOSE OF
COUNTERING SERIOUS CRIME

**Agreement between the Government of the United States of America and the
Government of Australia on Access to Electronic Data for the Purpose of
Countering Serious Crime**

The Government of the United States of America and the Government of Australia (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

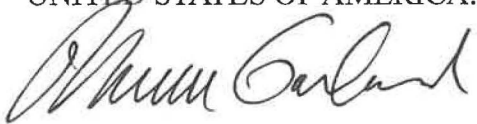
1. This Agreement shall remain in force for a five year period. The Parties may agree in writing to extensions of the Agreement.

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 Washington this 15th day of December, 2021 in duplicate, in the English language.

FOR THE GOVERNMENT OF THE
UNITED STATES OF AMERICA:



FOR THE GOVERNMENT OF
AUSTRALIA:





**THE HON KAREN ANDREWS MP
MINISTER FOR HOME AFFAIRS**

Dear Attorney General Garland,

I have the honour to refer to your letter dated 15 December 2021, regarding 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 Agreement”), signed today, which reads as follows:

I have the honor to refer to the Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime (“the Agreement”), signed today, and to propose that the Agreement be applied according to the following understandings.

The United States commits to inform Australia if it intends to invoke the Agreement to target data for the purpose of obtaining evidence or information to support or justify the detention of a current detainee held under law-of-war detention at Guantanamo Bay, Cuba, or a person nominated for, or designated for, such detention at Guantanamo, or for the purpose of obtaining evidence for use in a proceeding before a military commission at Guantanamo.

In addition, the United States commits to inform Australia if the United States Department of Defense intends to use data known by relevant Department personnel to have been obtained pursuant to Legal Process, as defined by the Agreement, as evidence in the prosecution’s case in military commission proceedings at Guantanamo, as information to be used against a detainee in reviews of such detention at Guantanamo, as evidence in support of the United States’ case in any legal proceedings challenging the Department’s authority to detain a current or nominated Guantanamo detainee, or as intelligence in support of military detention operations where the target of the operations has been nominated for, or designated for, detention at Guantanamo.

If the above proposal is acceptable to your Government, I have the honor to propose that this letter and your affirmative letter in reply would constitute an understanding between our two Governments as to the application of the Agreement, which would be operative on the date of entry into force of the Agreement.

On behalf of the Government of Australia, I am pleased to convey that your proposal is acceptable. Your letter and this reply constitute an understanding of our two Governments as to the application of the Agreement, which would be operative on the date of entry into force of the Agreement.

Sincerely,

A handwritten signature in cursive script, appearing to read "Karen Andrews".

KAREN ANDREWS

15 / 12 / 2021



**THE HON KAREN ANDREWS MP
MINISTER FOR HOME AFFAIRS**

Dear Attorney General Garland,

I have the honour to refer to your letter dated 15 December 2021, regarding 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 Agreement”), signed today, which reads as follows:

I have the honor to refer to the Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime (“the Agreement”), signed today, and to propose that Article 9(4) of the Agreement be interpreted and applied according to the following understandings.

The United States declares that its essential interests under the Agreement may be implicated by the introduction of data received pursuant to Legal Process, as defined by the Agreement, as evidence in the prosecution’s case in Australia in a manner that raises freedom of speech concerns for the United States, as further described in this letter. Accordingly, in the event that authorities in Australia receive data pursuant to such Legal Process and intend to introduce such data as evidence in the prosecution’s case in a manner that may raise those freedom of speech concerns, the Designated Authority of Australia is required to obtain permission from the Designated Authority of the United States prior to any use of the data in a manner that is or could be contrary to those essential interests, as described in Article 9(4).

The United States declares that the introduction of data received pursuant to Legal Process, as defined by the Agreement, as evidence in an Australian prosecution for certain offenses may raise freedom of speech concerns for the United States, depending on the facts of the case. Therefore, the Designated Authority of Australia should consult with and obtain permission from the Designated Authority of the United States prior to introducing such data as evidence in the prosecution’s case for any offense as to which conduct constituting any of the following is part of the basis for the offense charged:

- *Advocating terrorism or genocide.*
- *Membership in a terrorist organization.*
- *Associating with a terrorist organization in the context of conduct that does not involve the provision of material support or resources.*
- *Advocating or inciting violence in circumstances not involving imminent or actual harm.*
- *Racial vilification or harassment.*
- *Defamation.*
- *Using a service to menace, harass or cause offence, in the context of both the making or publishing of statements.*
- *Unauthorized disclosure of information in the context of activities that are journalistic in nature.*
- *Failing to remove, or ceasing to host, abhorrent violent material.*

Any other federal, state or territory offenses analogous to the above categories, including those that relate to anticipatory offenses, should also be treated as though they have been included in the list.

In addition to offenses listed above, prosecutions for other offenses also may raise freedom of speech concerns for the United States, depending on the facts of the case, such as prosecutions for conduct involving news gathering and publication, or public protest. The Designated Authority of Australia should thus consult with the Designated Authority of the United States when Australian officials intend to introduce data received pursuant to Legal Process, as defined by the Agreement, as evidence in the prosecution's case in relation to an offense category not listed above and such officials have reason to believe, based on the context of the case and their understanding of U.S. views—including Australia's experience with U.S. views expressed in the mutual legal assistance process—that the introduction of the data as evidence in the prosecution's case may raise freedom of speech concerns for the United States. As set out in Article 9(4), if the Designated Authority of the United States confirms that there are freedom of speech concerns that cannot be resolved by the imposition of conditions, such data will not be introduced as evidence in the prosecution's case.

In addition to the prosecutions described above that may raise freedom of speech concerns for the United States, prosecutions under Australia's control order and extended supervision order regimes also may implicate the same concerns and, therefore, should be dealt with in the same manner. Accordingly, when authorities in Australia intend to introduce data obtained pursuant to Legal Process, as defined by the Agreement, as evidence in the prosecution's case for the violation of such orders, where that violation is based in substantial part on speech, the Designated Authority of Australia should consult with the Designated Authority of the United States. As set out in Article 9(4), if the Designated Authority of the United States confirms that there are freedom of speech concerns that cannot be resolved by the imposition of conditions, such data will not be introduced as evidence in the prosecution's case.

The United States may unilaterally supplement the categories of offenses set forth above if offenses in other Australian federal, state or territory statutes, either applied currently or those that may be enacted in future, merit inclusion. Any such supplement to this letter is effective on the date of a written notification from the Designated Authority of the United States to the Designated Authority of Australia notifying it thereof.

If the foregoing is acceptable to your Government, I have the honor to propose that this letter and your affirmative letter in reply would constitute an understanding between our two Governments as to the interpretation and application of the Agreement, which would be operative on the date of entry into force of the Agreement.

On behalf of the Government of Australia, I am pleased to convey that your proposal is acceptable. Your letter and this reply constitute an understanding of our two Governments as to the interpretation and application of the Agreement, which would be operative on the date of entry into force of the Agreement.

Sincerely,



KAREN ANDREWS

15 / 12 / 2021



**THE HON KAREN ANDREWS MP
MINISTER FOR HOME AFFAIRS**

Dear Attorney General Garland,

I have the honour to refer 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 ("the Agreement"), signed today, and to propose that Article 9(4) of the Agreement be interpreted and applied according to the following understandings.

Australia declares that its essential interests under the Agreement may be implicated by the introduction of data received pursuant to Legal Process, as defined by the Agreement, as evidence in the prosecution's case in the United States for an offence for which the death penalty is sought. Accordingly, in the event that authorities in the United States receive such data and intend to introduce such data as evidence in the prosecution's case for an offence for which the death penalty is sought, the Designated Authority of the United States is required to obtain permission from the Designated Authority of Australia prior to any use of the data in a manner that is or could be contrary to those essential interests, as described in Article 9(4).

If the above is acceptable to your Government, I have the honour to propose that this letter and your affirmative letter in reply would constitute an understanding between our two Governments as to the interpretation and application of the Agreement, which would be operative on the date of entry into force of the Agreement.

Sincerely,

A handwritten signature in black ink, appearing to read 'Karen Andrews'.

KAREN ANDREWS

15 / 12 / 2021



Office of the Attorney General
Washington, D. C. 20530

Dear Minister Andrews,

I have the honor to refer to the Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime (“the Agreement”), signed today, and to propose that the Agreement be applied according to the following understandings.

The United States commits to inform Australia if it intends to invoke the Agreement to target data for the purpose of obtaining evidence or information to support or justify the detention of a current detainee held under law-of-war detention at Guantanamo Bay, Cuba, or a person nominated for, or designated for, such detention at Guantanamo, or for the purpose of obtaining evidence for use in a proceeding before a military commission at Guantanamo.

In addition, the United States commits to inform Australia if the United States Department of Defense intends to use data known by relevant Department personnel to have been obtained pursuant to Legal Process, as defined by the Agreement, as evidence in the prosecution’s case in military commission proceedings at Guantanamo, as information to be used against a detainee in reviews of such detention at Guantanamo, as evidence in support of the United States’ case in any legal proceedings challenging the Department’s authority to detain a current or nominated Guantanamo detainee, or as intelligence in support of military detention operations where the target of the operations has been nominated for, or designated for, detention at Guantanamo.

If the above proposal is acceptable to your Government, I have the honor to propose that this letter and your affirmative letter in reply would constitute an understanding between our two Governments as to the application of the Agreement, which would be operative on the date of entry into force of the Agreement.

Sincerely,

A handwritten signature in black ink, appearing to read "Merrick B. Garland".

Merrick B. Garland
Attorney General

12/15/2021



Office of the Attorney General
Washington, D. C. 20530

Dear Minister Andrews,

I have the honor to refer to your letter dated December 15, 2021, regarding the Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime (“the Agreement”), signed today, which reads as follows:

I have the honour to refer 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 (“the Agreement”), signed today, and to propose that Article 9(4) of the Agreement be interpreted and applied according to the following understandings.

Australia declares that its essential interests under the Agreement may be implicated by the introduction of data received pursuant to Legal Process, as defined by the Agreement, as evidence in the prosecution’s case in the United States for an offence for which the death penalty is sought. Accordingly, in the event that authorities in the United States receive such data and intend to introduce such data as evidence in the prosecution’s case for an offence for which the death penalty is sought, the Designated Authority of the United States is required to obtain permission from the Designated Authority of Australia prior to any use of the data in a manner that is or could be contrary to those essential interests, as described in Article 9(4).

If the above is acceptable to your Government, I have the honour to propose that this letter and your affirmative letter in reply would constitute an understanding between our two Governments as to the interpretation and application of the Agreement, which would be operative on the date of entry into force of the Agreement.

On behalf of the Government of the United States of America, I am pleased to convey that your proposal is acceptable. Your letter and this reply constitute an understanding of our two Governments as to the interpretation and application of the Agreement, which would be operative on the date of entry into force of the Agreement.

Sincerely,

Merrick B. Garland
Attorney General

12/15/2021



Office of the Attorney General
Washington, D. C. 20530

Dear Minister Andrews,

I have the honor to refer to the Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime (“the Agreement”), signed today, and to propose that Article 9(4) of the Agreement be interpreted and applied according to the following understandings.

The United States declares that its essential interests under the Agreement may be implicated by the introduction of data received pursuant to Legal Process, as defined by the Agreement, as evidence in the prosecution’s case in Australia in a manner that raises freedom of speech concerns for the United States, as further described in this letter. Accordingly, in the event that authorities in Australia receive data pursuant to such Legal Process and intend to introduce such data as evidence in the prosecution’s case in a manner that may raise those freedom of speech concerns, the Designated Authority of Australia is required to obtain permission from the Designated Authority of the United States prior to any use of the data in a manner that is or could be contrary to those essential interests, as described in Article 9(4).

The United States declares that the introduction of data received pursuant to Legal Process, as defined by the Agreement, as evidence in an Australian prosecution for certain offenses may raise freedom of speech concerns for the United States, depending on the facts of the case. Therefore, the Designated Authority of Australia should consult with and obtain permission from the Designated Authority of the United States prior to introducing such data as evidence in the prosecution’s case for any offense as to which conduct constituting any of the following is part of the basis for the offense charged:

- Advocating terrorism or genocide.
- Membership in a terrorist organization.
- Associating with a terrorist organization in the context of conduct that does not involve the provision of material support or resources.
- Advocating or inciting violence in circumstances not involving imminent or actual harm.
- Racial vilification or harassment.
- Defamation.
- Using a service to menace, harass or cause offence, in the context of both the making or publishing of statements.

- Unauthorized disclosure of information in the context of activities that are journalistic in nature.
- Failing to remove, or ceasing to host, abhorrent violent material.

Any other federal, state or territory offenses analogous to the above categories, including those that relate to anticipatory offenses, should also be treated as though they have been included in the list.

In addition to offenses listed above, prosecutions for other offenses also may raise freedom of speech concerns for the United States, depending on the facts of the case, such as prosecutions for conduct involving news gathering and publication, or public protest. The Designated Authority of Australia should thus consult with the Designated Authority of the United States when Australian officials intend to introduce data received pursuant to Legal Process, as defined by the Agreement, as evidence in the prosecution's case in relation to an offense category not listed above and such officials have reason to believe, based on the context of the case and their understanding of U.S. views—including Australia's experience with U.S. views expressed in the mutual legal assistance process—that the introduction of the data as evidence in the prosecution's case may raise freedom of speech concerns for the United States. As set out in Article 9(4), if the Designated Authority of the United States confirms that there are freedom of speech concerns that cannot be resolved by the imposition of conditions, such data will not be introduced as evidence in the prosecution's case.

In addition to the prosecutions described above that may raise freedom of speech concerns for the United States, prosecutions under Australia's control order and extended supervision order regimes also may implicate the same concerns and, therefore, should be dealt with in the same manner. Accordingly, when authorities in Australia intend to introduce data obtained pursuant to Legal Process, as defined by the Agreement, as evidence in the prosecution's case for the violation of such orders, where that violation is based in substantial part on speech, the Designated Authority of Australia should consult with the Designated Authority of the United States. As set out in Article 9(4), if the Designated Authority of the United States confirms that there are freedom of speech concerns that cannot be resolved by the imposition of conditions, such data will not be introduced as evidence in the prosecution's case.

The United States may unilaterally supplement the categories of offenses set forth above if offenses in other Australian federal, state or territory statutes, either applied currently or those that may be enacted in future, merit inclusion. Any such supplement to this letter is effective on the date of a written notification from the Designated Authority of the United States to the Designated Authority of Australia notifying it thereof.

If the foregoing is acceptable to your Government, I have the honor to propose that this letter and your affirmative letter in reply would constitute an understanding between our two Governments as to the interpretation and application of the Agreement, which would be operative on the date of entry into force of the Agreement.

Sincerely,

A handwritten signature in black ink, appearing to read "Merrick Garland". The signature is fluid and cursive, with a large initial "M" and a long, sweeping underline.

Merrick B. Garland
Attorney General

12/15/2021



Office of the Attorney General
Washington, D. C. 20530

December 15, 2021

On December 15, 2021, the Minister for Home Affairs of Australia and I signed the Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime. A signed copy of the Agreement is attached.

I hereby certify my determination that the Agreement satisfies the requirements of Section 2523(b) of Title 18 of the U.S. Code. My determination is based on the considerations in paragraphs (1), (2), (3), and (4) of Section 2523(b), as explained in the attached document prepared by attorneys at the U.S. Department of Justice in consultation with U.S. Department of State. Secretary of State Blinken has concurred with this determination.

Sincerely,

A handwritten signature in black ink, appearing to read "Merrick B. Garland", written over a horizontal line.

Merrick B. Garland
Attorney General of the United States

Explanation of Each Consideration in Determining that the Agreement Satisfies the Requirements of 18 U.S.C. § 2523(b)

The Attorney General, with the concurrence of the Secretary of State, has determined and certified that the Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, signed at Washington, D.C., on the 15th of December, 2021 (“the Agreement”) satisfies the requirements of 18 U.S.C. § 2523(b), including each consideration in paragraphs (1), (2), (3), and (4) of Section 2523(b). Further explanation in support of this determination is provided below.

18 U.S.C. § 2523(b)(1)

With respect to the considerations listed in 18 U.S.C. § 2523(b)(1), the domestic law of Australia, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of Australia that will be subject to the Agreement.

This explanation takes into account credible information and expert input. This includes expertise within the U.S. government, consultations with U.S.- and Australia-based academics and civil society organizations,¹ as well as a consideration of publicly available information, including but not limited to the Department of State, Bureau of Democracy, Human Rights, and Labor 2020 Country Report on Human Rights Practices: Australia (the “Australia Human Rights Report”). These consultations and the information reviewed indicate that Australia is an appropriate partner for an agreement under the Clarifying Lawful Overseas Use of Data Act, Div. V, Consolidated Appropriations Act, 2018, P.L. 115-141, 28 U.S.C. 2523(b) (2018) (“the CLOUD Act”).

General Protections

Australia demonstrates strong respect for human rights in its domestic laws and policies and is a strong advocate for a rules-based international system and the protection of human rights globally. Australia is party to seven United Nations human rights treaties, including the International Covenant on Civil and Political Rights, the International Convention on the Elimination of all Forms of Racial Discrimination, and the Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment. It is also party to several United Nations optional protocols, including the Optional Protocol of the Convention against Torture and other

¹ Consistent with the CLOUD Act, the Department of Justice and the Department of State consulted with members of Australian and American civil society organizations. These individuals raised a range of points and concerns about, *inter alia*, the scope and implementation of Australian criminal and national security legislation, with a particular focus on the Telecommunications Legislation Amendment (International Production Orders) Act 2021. Points were also raised about the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (also known as the TOLA Act 2018) and control orders imposed under Criminal Code Act 1995 Division 104. These concerns were taken into consideration in reaching the conclusions of this determination and certification.

Cruel, Inhuman or Degrading Treatment or Punishment. Australia has adopted legislation and policies to give effect to its obligations under these treaties.

All Australian legislation introduced in the Australian Parliament is required by law to include a Statement of Compatibility with the rights and freedoms recognized in the seven international human rights treaties that Australia has ratified. The Australian Human Rights Commission is an independent organization established by the Australian Parliament that investigates complaints of discrimination or breaches of human rights under federal laws that implement Australia's human rights treaty obligations.

Australia is a leader on human rights in multilateral forums, including the United Nations General Assembly and the Human Rights Council. It engages constructively in the Universal Periodic Review Process as well as in other human rights-related processes mechanisms, including United Nations Special Procedures.

18 U.S.C. § 2523(b)(1)(B)(i) Australia has adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated by being a party to the Convention on Cybercrime, done at Budapest on November 23, 2001, or through domestic laws that are consistent with definitions and the requirements set forth in chapters I and II of that Convention.

Australia is a party to the Convention on Cybercrime, done at Budapest on November 23, 2001 (the "Budapest Convention"). Australia became fully compliant with the Budapest Convention with the Cybercrime Legislation Amendment Act 2012, which amended provisions of the Telecommunications (Interception and Access) Act 1979 (TIA Act), Criminal Code Act 1995 (Criminal Code), the Telecommunications Act 1997, and the Mutual Assistance in Criminal Matters Act 1987. Australia ratified the Budapest Convention on November 30, 2012, with entry into force on March 1, 2013.

18 U.S.C. § 2523(b)(1)(B)(ii) Australia demonstrates respect for the rule of law and principles of non-discrimination.

Australia demonstrates respect for the rule of law and principles of non-discrimination. Australia is a constitutional democracy with a freely elected federal parliamentary government. Covering Clause 5 to the Australian Constitution provides that "all laws made by the Parliament of the Commonwealth under the Constitution, shall be binding on the courts, judges and people of every State and of every part of the Commonwealth." The rule of law is given effect by an independent and impartial federal judiciary established under Chapter III of the Australian Constitution. Australia's respect for principles of non-discrimination is incorporated into its domestic law through the Racial Discrimination Act 1975, Sex Discrimination Act 1984, Disability Discrimination Act 1992, and Age Discrimination Act 2004. Complaints made under these laws are investigated by the Australian Human Rights Commission. In addition, the Fair Work Act 2009 protects against discrimination by private employers and is enforced by the Fair Work Ombudsman, an independent statutory office. If the Australian Human Rights Commission or Fair Work Ombudsman do not resolve the complaints, the complainant may apply to the Federal Court of Australia or the Federal Circuit Court of Australia.

As reported in the Department of State’s 2020 Country Report on Human Rights Practices for Australia (“Australia Human Rights Report”):

[Australian] law provides the same legal status and rights for women as for men, including under laws related to family, religion, personal status, labor, property, nationality, and inheritance, as well as employment, credit, pay, owning or managing businesses, education, and housing. The government enforced the law effectively. Employment discrimination against women occurred, and there was a much-publicized “gender pay gap.”

....

The law prohibits discrimination against persons with physical, sensory, intellectual, and mental disabilities. The government effectively enforced the law.

....

No laws criminalize consensual same-sex sexual conduct between adults. Discrimination based on sexual orientation and gender identity is prohibited by law in a wide range of areas, including employment, housing, family law, taxes, child support, immigration, pensions, care of elderly persons, and social security. The law provides protections against discrimination based on sexual orientation, gender identity, and sex characteristics.

....

Federal, state, and territory laws provide for protections against employment discrimination.

Australian law prohibits discrimination and individuals have rights under applicable law to challenge discrimination, including through the Australian Human Rights Commission, the Fair Work Ombudsman, and the independent judiciary.

18 U.S.C. § 2523(b)(1)(B)(iii) Australia adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights including –

(I) protection from arbitrary and unlawful interference with privacy.

As reported in the Australia Human Rights Report, Australian law prohibits arbitrary or unlawful interference with privacy, family, the home, or correspondence, and there were no reports the government failed to respect these prohibitions. The primary law protecting the personal information of individuals in Australia is the Privacy Act 1988 (“Privacy Act”). This Act applies to Australian Government agencies and private sector organizations with an annual turnover of more than 3 million Australian dollars and to organizations providing certain services that deal in more sensitive personal information such as health care services and credit reporting (“APP entities”). Some, but not all, Australian states and territories have similar legislation governing state and territorial government agencies. The Office of the Australian Information Commissioner is responsible for investigating breaches of the Privacy Act and regulating compliance. Individuals may seek judicial – and, in some instances, merits – review of the decisions and determinations of the Australian Information Commissioner.

The Privacy Act establishes thirteen privacy principles (“Australian Privacy Principles” or APPs) that govern the collection, use, and disclosure of personal information by APP entities, as well as the rights of individuals to access and correct their personal information and the accountability of APP entities. In particular, APP entities, including Australian Government law enforcement, must only collect personal information by lawful and fair means and must not collect personal information “unless the information is reasonably necessary for, or directly related to, one or more of the entity’s functions or activities.” Personal information may not be used or disclosed for a purpose other than the purpose for which it was collected unless an exception applies. Exceptions include where: the individual consents to additional uses or disclosures; the individual would reasonably expect the use or disclosure for the secondary purpose and the secondary purpose relates to the primary purpose; the secondary use or disclosure is reasonably necessary for law enforcement activities; or the additional use or disclosure is allowed based on a permitted situation, Australian law, or court order.

In addition, the Telecommunications Act 1997 prohibits telecommunications service providers from disclosing information or documents relating to the contents or substance of communications that have been or are being carried by the provider, or the affairs or personal particulars of another person except as specifically authorized. The statute specifically authorizes disclosure or use of such information where required or authorized by or under law, including in response to a warrant in connection with the operation of an enforcement agency.

Electronic surveillance is further regulated by the TIA Act, which prohibits intercepting communications and accessing stored communications, subject to certain limited exceptions that permit law enforcement and other agencies to apply for warrants to intercept communications and access stored communications when investigating serious crimes or threats to national security.

The Telecommunications Legislation Amendment (International Production Orders) Act 2021 (“IPO Act”) creates domestic authority to seek orders for disclosure of electronic data from communications providers in connection with the investigation of a serious crime or for national security purposes, pursuant to a designated international agreement. For international production orders (“IPOs”) relating to criminal law violations, the issuing authority must have regard to, among other things, how much the privacy of any person or persons would be likely to be interfered with under the order and the extent to which other methods have been used or are available to the requesting agency, as well as the gravity of the conduct, the potential prejudice to the investigation which might arise from alternate methods to seek the requested information, and how much the requested information would be likely to assist in connection with the investigation. Where IPOs relate to national security, the issuing authority must have regard to, among other things, the extent to which there are other less intrusive methods available and the degree to which those other methods would effectively substitute for the order or cause prejudice to national security.

(II) fair trial rights.

According to the Australia Human Rights Report:

[Australian] law provides for the right to a fair and timely public trial, and an independent judiciary generally enforced this right. In state district and county courts, and in state and territorial supreme courts, a judge and jury try serious offenses. Defendants enjoy a presumption of innocence and cannot be compelled to testify or confess guilt. They have the right to be informed promptly and in detail of the charges, with free interpretation as necessary from the moment charged through all appeals, the right to an attorney, to be present at their trial, and adequate time and facilities to prepare a defense. Government-funded attorneys are available to low-income persons. The defendant's attorney can question witnesses, present witnesses and evidence, and appeal the court's decision or the sentence imposed.

The Criminal Code requires in Part 2.6 that "the prosecution bears a legal burden of proving every element of an offense relevant to the guilt of the person charged" as well as "a legal burden of disproving any matter in relation to which the defendant has discharged an evidential burden of proof imposed on the defendant." The standard for the prosecution is proof beyond a reasonable doubt, unless the offense otherwise specifies a different standard of proof.

(III) freedom of expression, association, and peaceful assembly.

Australia has a strong tradition respecting freedom of expression and promoting a free press. As reported in the Australia Human Rights Report:

Although the [Australian] constitution does not explicitly provide for freedom of speech or press, the High Court has held that the constitution implies a limited right to freedom of political expression, and the government generally respected this right. An independent press, an effective judiciary, and a functioning democratic political system combined to promote freedom of expression, including for the press.

....

There were no government restrictions on academic freedom or cultural events.

....

Although the freedoms of peaceful assembly and association are not codified in federal law, the government generally respected these rights.

Regarding political expression, the implied freedom of political expression in the Australian Constitution means that any law burdening the freedom must be reasonably appropriate and adapted to serve a legitimate end, in the sense that its purpose and the means adopted are compatible with the maintenance of the constitutionally prescribed system of representative and responsible government. *See McCloy v. New South Wales* [2015] HCA 34; *Coleman v. Power* [2004] HCA 39; *Lange v Australian Broadcasting Commission* [1997] HCA 25.

Like the United States, the Australian government has, from time to time, opened criminal investigations into leaks of classified information. One notable case involved an investigation related to the 2018 publication by News Corp of an article on surveillance of citizens that allegedly contained classified information. The Australian Federal Police executed a warrant on the home of the journalist in 2019. The highest federal court later found that the warrant was invalid, however. The Australian Federal Police finalized the investigation without filing charges. A second investigation of a journalist involved Australian Broadcasting Corporation (ABC) news reports published in 2017 alleging that Australia had committed war crimes in Afghanistan. The Australian Federal Police executed a search warrant in June 2019 at ABC's Sydney headquarters.

As described in the Australia Human Rights Report, these actions:

sparked a national discussion on press freedom, led by a coalition of media organizations calling for more legal protections for journalists and whistleblowers. In August [of 2019] the Parliamentary Joint Committee on Intelligence and Security released a report into "the impact of the exercise of law enforcement and intelligence powers on the freedom of the press." The committee's inquiry was initiated by the federal attorney general following public concerns about the two federal police raids. The committee recommended the government make changes to the use of warrants that would establish a "public interest advocate" to contest the issuance of warrants against journalists and media organizations. Media organizations including News Corp and the ABC said the report did not go far enough and continued to seek the ability to contest warrants themselves before raids take place.

Subsequent to the publication of the Parliamentary Joint Committee on Intelligence and Security's report, the Australian government tabled a response in December 2020, in which it agreed or agreed in principle to all fifteen recommendations directed at the government. At this time, the Australian government is in the process of implementing these recommendations.

Australian criminal laws sometimes cover speech acts not contained in U.S. law. Certain Australian laws, such as the Criminal Code Act 1995, Part 10.6, Division 474, Subdivision H, are broadly worded and may criminalize expression that in the United States would be considered protected speech under the First Amendment. In addition, the Online Safety Act 2021, passed by the Australian parliament in June 2021, sets forth plans for online safety measures to combat cyber bullying, cyber abuse, and the non-consensual sharing of intimate images of a person. Under the law, Australia's eSafety Commissioner has the authority to issue removal notices for these types of content and can also request or require internet service providers to block access to material that promotes, incites, instructs, or depicts "abhorrent violent conduct." While much of this conduct would likely violate similar criminal laws in the United States (and prosecution would not be barred by the First Amendment), some conduct covered by these statutes may fall outside of what could be prohibited consistent with the First Amendment.

No country has implemented legal protections for freedom of expression, association, and peaceful assembly in as expansive a manner as the United States pursuant to the First

Amendment and other laws. However, despite these differences between the legal protections provided for in Australia and the United States, Australia maintains effective legal protections for freedom of expression, association, and peaceful assembly, as discussed in the Australia Human Rights Report.

(IV) prohibitions on arbitrary arrest and detention.

According to the Australia Human Rights Report:

[Australian law] prohibits arbitrary arrest and detention, and the government generally observed these prohibitions.

....

Police must inform arrested persons immediately of their legal rights and the grounds for their arrest and must bring arrested persons before a magistrate for a bail hearing at the next session of the court. The maximum investigation period police may hold and question a person without charge is 24 hours, unless extended by a court order for up to an additional 24 hours.

Under limited circumstances in terrorism cases, a number of federal and state or territorial laws permit police to hold individuals in preventative detention without charge or questioning for up to 14 days. These laws contain procedural safeguards including on access to information related to lawyer-client communication.

....

The law allows courts to detain convicted terrorists beyond the expiration of their sentence by up to an additional three years for preventive purposes where there is no less restrictive measure available to prevent the risk posed by the offender to the community.

And while some have criticized this aspect of the law as allowing the government to detain prisoners indefinitely and arbitrarily, it bears noting that Australian law places the power to extend sentences of convicted terrorists in the independent judiciary.

(V) prohibitions against torture and other cruel, inhuman, or degrading treatment or punishment.

As reported in the Australia Human Rights Report, Australian law prohibits torture and other cruel, inhuman, or degrading treatment or punishment, and the government generally respected these provisions, though there were occasional claims that police and prison officials mistreated suspects in custody.

Australia is a party to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT). Australia is also a party to the International Covenant on Civil and Political Rights, which prohibits torture and cruel, inhuman or degrading treatment or punishment. Torture by those acting in an official capacity is a criminal offense in Australia under Division 274 of the Criminal Code, with a maximum penalty of twenty years imprisonment. Section 23Q of the Crimes Act 1914 requires that a “person who is under arrest or

a protected suspect must be treated with humanity and with respect for human dignity, and must not be subjected to cruel, inhuman, or degrading treatment.”

Australia submitted its 6th periodic report under the CAT in January 2019, which responded to points raised by the UN Committee against Torture in its assessment of Australia’s 4th and 5th reports.² The UN Committee against Torture has not to date concluded its consideration of the report.

18 U.S.C. § 2523(b)(1)(B)(iv): Australia has clear legal mandates and procedures governing those Australian entities that are authorized to seek data under the Agreement, including procedures through which those authorities collect, retain, use, and share data, and effective oversight of these activities.

The Australian entities authorized to seek data under the Agreement may do so under new legislation passed in June 2021: the IPO Act, which governs interception and acquisition of live and stored communications and metadata from overseas providers. Together with the Privacy Act and the Inspector-General of Intelligence and Security Act 1986, the IPO Act establishes the procedures through which Australian agencies collect, retain, use, and share data under the Agreement, as well as provide for effective oversight of these activities.

Telecommunications Legislation Amendment (International Production Orders) Act 2021 (IPO Act)

The IPO Act sets forth procedures for obtaining orders to intercept communications and to compel production of stored communications or non-content communications data for criminal and national security purposes.³ The IPO Act identifies the public authorities, including law enforcement and intelligence agencies, that may apply for orders under the Act.⁴ It sets the legal standards that must be met for an agency to apply for an order to an issuing authority.⁵ It specifies that the issuing authority is either an eligible judicial officer or a nominated member of the Administrative Appeals Tribunal (“AAT”) and it outlines the factors that must be considered by the issuing authority before an order is issued.⁶ The IPO Act also establishes an Australian Designated Authority to review orders for compliance with the designated international agreement nominated in the application for the order.⁷ The IPO Act prohibits the use or disclosure of data collected unless certain statutorily enumerated exceptions apply, including for the investigation of serious crimes, the performance of intelligence functions, and for oversight

² Available at <https://www.ag.gov.au/sites/default/files/2020-03/integrity-human-rightscat-report.PDF>.

³ See IPO Act Part 2 (international production orders relating to the enforcement of the criminal law); Part 3 (international production orders relating to control orders); Part 4 (international production orders relating to national security).

⁴ See *id.* § 22 (criminal law IPOs), § 52 (control order IPOs), § 83 (national security IPOs).

⁵ *Id.* Subdivisions A of Parts 2, 3 and 4.

⁶ See *id.* Subdivisions B of Parts 2, 3 and 4. The AAT is an independent statutory body that conducts independent merits review of administrative decisions made under approximately 400 Commonwealth laws. Some AAT members are also judges. See About the AAT, available at <https://www.aat.gov.au/about-the-aat>.

⁷ *Id.* §§ 111-112.

purposes.⁸ In addition, agencies are also required to destroy data where it is not likely to be required for a permitted purpose.⁹ The Privacy Act, as explained further below, governs access, use, and retention of personal data by Commonwealth authorities, including such data collected under the IPO Act.

Compliance with the IPO Act is subject to review and oversight by the Commonwealth Ombudsman. The Commonwealth Ombudsman is empowered to inspect the records of law enforcement agencies authorized to use the IPO Act and records of the Australian Designated Authority to audit compliance with the Act and each year must report on the results of its inspections to the Minister of Home Affairs.¹⁰ The Commonwealth Ombudsman is appointed by the Governor-General of Australia for up to seven years and is eligible for reappointment after this term,¹¹ and is removable by the Governor-General for excessive absence from duty, financial insolvency, or following a request by both Houses of Parliament on the grounds of misbehavior or physical or mental incapacity.¹²

The Privacy Act 1988

The Privacy Act regulates the collection, storage, security, use, disclosure, and integrity of personal data held by Commonwealth agencies, but does not cover intelligence agencies.¹³ Under the Privacy Act, personal data must be collected directly from the individual to whom it relates, unless: for Government agencies, the individual consents to the collection from a third party or the collection from a third party is authorized by an Australian law or a court or tribunal order; or for all entities subject to the Act, it is unreasonable or impracticable to collect it from the individual.¹⁴ Government agencies may only collect personal information (other than sensitive information) that is “reasonably necessary for, or directly related to, one or more of the agency’s functions or activities.”¹⁵ Absent a specified exception, sensitive information (*e.g.*, information regarding an individual’s racial or ethnic origin, political opinions, religious beliefs, or health) may be collected only if the individual consents and it is reasonably necessary for one or more of the entity’s functions or activities, and this information may not be used or disclosed for a secondary purpose unless that purpose is directly related to the primary purpose of collection and within the reasonable expectations of the individual.¹⁶

Agencies must take such steps as are reasonable under the circumstances to notify individuals that their personal information has been collected at or before the time of collection, or as soon as practicable afterwards.¹⁷ Personal information collected for a particular purpose may not be used or disclosed for another purpose except as specified under the statute, including as

⁸ *Id.* §§ 140, 152-153.

⁹ *Id.* §140.

¹⁰ *Id.* §§ 142-150. Inspection reports are available at <https://www.ombudsman.gov.au/publications/reports/inspection/all-reports>.

¹¹ Ombudsman Act 1976 § 22.

¹² *Id.* § 28.

¹³ Privacy Act 1988 § 7(1)(f), (1A).

¹⁴ Privacy Act, Schedule I, Privacy Principle 3.6.

¹⁵ *Id.* 3.1.

¹⁶ *Id.* 3.3, 3.4.

¹⁷ *Id.* 5.1.

reasonably necessary for enforcement-related activities of law enforcement bodies.¹⁸ Reasonable steps under the circumstances must be taken to ensure the personal information collected, used or disclosed by a government agency is accurate, up-to-date, complete, and relevant to any use or disclosure.¹⁹ Personal information held by government agencies must be protected from misuse, interference, loss, and unauthorized access, modification, or disclosure through such steps as are reasonable under the circumstances.²⁰ In addition, government agencies shall take reasonable steps under the circumstances to destroy or de-identify personal information no longer needed for any purpose or required to be held under Australian law, due to a court or tribunal order, or for Commonwealth records purposes.²¹ Individuals shall have access to their personal information held by a government agency unless Australian law authorizes the agency to refuse access.²² Individuals may also request corrections to their personal information held by a government agency under the Privacy Act.²³ If the agency refuses to correct the record, it must provide the individual with written notice for the reasons for the refusal, except to the extent that it would be unreasonable to do so.²⁴

Compliance with the Privacy Act, including compliance by law enforcement agencies, is overseen by the Australian Information Commissioner.²⁵ The Information Commissioner investigates complaints of violations of the Privacy Act and has the power to issue court-enforceable determinations to agencies to resolve such complaints.²⁶ She may also investigate agency practices under the Privacy Act on her own initiative²⁷ or direct government agencies to provide privacy impact assessments on their activities or functions which may have a significant impact on the privacy of individuals or involve the handling of personal information.²⁸

The Inspector-General of Intelligence and Security Act 1986

The Inspector-General of Intelligence and Security (“IGIS”) is an independent statutory office holder who reviews the activities of Australian intelligence agencies, including the Australian Security Intelligence Organization (“ASIO”), to ensure that the agencies act legally and with propriety, comply with ministerial guidelines and directives, and respect human rights. As established by the Inspector-General of Intelligence and Security Act 1986, the IGIS is appointed by the Governor-General, based upon a recommendation from the Prime Minister in with consultation with the Leader of the Opposition.²⁹ The IGIS is authorized to review matters that

¹⁸ *Id.* 6.2.

¹⁹ *Id.* 10.1, 10.2.

²⁰ *Id.* 11.1.

²¹ *Id.* 11.2.

²² *Id.* 12.1, 12.2, 12.3.

²³ *Id.* 13.1.

²⁴ *Id.* 13.3.

²⁵ *Id.* Part IV. Because the Privacy Act excludes intelligence agencies, the Australian Information Commissioner does not have authority over intelligence agencies. The Inspector General of Intelligence and Security oversees intelligence agency activities.

²⁶ *Id.* Division 1

²⁷ *Id.* Division 3.

²⁸ *Id.* Division 3A.

²⁹ Inspector-General of Intelligence and Security Act 1986, § 6.

relate to these agencies' activities, including those related to the IPO Act.³⁰ The IGIS may act upon its own initiative, upon requests from the Prime Minister and other senior officials, or upon complaints from the public.³¹ Additionally, the IGIS can conduct inspections of intelligence agency activities as it deems appropriate.³²

18 U.S.C. § 2523(b)(1)(B)(v): Australia has sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data.

Australian law and the oversight and reporting requirements mandated by the text of the Agreement are the primary elements relevant to ensuring accountability and transparency with regard to Australia's collection and use of electronic data collected pursuant to the Agreement. Data obtained by an Australian law enforcement or intelligence agency using an IPO must be handled, used, and disclosed in accordance with the information protection provisions in Schedule 1 of the TIA Act and any applicable domestic privacy laws.

As explained above, the Privacy Act, Australian Privacy Principles, and equivalent state and territory privacy legislation and policies contain mechanisms to provide accountability and transparency regarding collection and use of electronic data. Australian Privacy Principle 1 outlines the requirements for managing personal information in an open and transparent way, including ensuring an APP entity takes reasonable steps under the circumstances to implement practices, procedures, and systems to comply with the Australian Privacy Principles and to enable it to address related inquiries and complaints.³³ Australian Privacy Principle 6 states that an APP entity generally may not use or disclose personal information for a purpose other than the purpose for which it was collected, unless the individual consents or a specified exception applies (*e.g.*, the use or disclosure is required or authorized by Australian law or court/tribunal order, or the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for an enforcement-related activity conducted by, or on behalf of, an enforcement body).³⁴

Part 9 of Schedule 1 of the TIA Act establishes the framework for reporting and record keeping for agencies that are consistent with the current domestic warrant regime. This includes annual reports by law enforcement agencies and the Australian Designated Authority on the use of IPOs³⁵ and a report from the Director-General of Security to the Attorney-General on the extent to which compliance with IPOs by communications providers has assisted ASIO in carrying out its functions.³⁶

³⁰ *Id.* § 8.

³¹ *Id.*

³² *Id.* § 9A.

³⁴ Privacy Act, Schedule 1, 1.2.

³⁴ *Id.* 6.1-6.2.

³⁵ IPO Act, §§ 128, 130.

³⁶ *Id.* § 129.

The Commonwealth Ombudsman, who has a significant existing role in supervising the use of covert, intrusive, and coercive law enforcement powers, will oversee the activities of law enforcement agencies and the Australian Designated Authority under the IPO Act framework through inspections and reporting.³⁷ The Commonwealth Ombudsman's annual inspection reports will be publicly tabled in each House of Parliament.³⁸

In addition, as noted above, the activities of Australia's Intelligence Community, including those relating to information obtained from IPOs, are subject to oversight by the IGIS.

Finally, Part 11 of Schedule 1 to the TIA Act makes it an offense to use, record, disclose, or admit into evidence information obtained in accordance with or about an IPO unless an exception applies.³⁹ Exceptions include, but are not limited to, uses, recordings, and disclosures for the purpose of investigating or prosecuting of relevant serious offenses,⁴⁰ making reports and keeping of records under Part 9,⁴¹ independent oversight by the Commonwealth Ombudsman⁴² and Inspector-General of Intelligence and Security,⁴³ and a designated international agreement.⁴⁴

18 U.S.C. § 2523(b)(1)(B)(vi) Australia demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet.

According to the Australia Human Rights Report:

The [Australian] government did not restrict or disrupt access to the internet or censor online content, and there were no credible reports that the government monitored private online communications without appropriate legal authority. The internet was widely available to and used by citizens. Law enforcement agencies require a warrant to intercept telecommunications, including internet communications.

In addition, Australia has no broad-based data localization laws, and has opposed the adoption by other countries of broad data localization laws.

18 U.S.C. § 2523(b)(2) Australia has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the Agreement.

³⁷ *Id.* §§ 142-43.

³⁸ *Id.* § 150.

³⁹ *Id.* §§ 152, 153.

⁴⁰ *Id.* §§ 153(1)(a)-(c).

⁴¹ *Id.* § 153(1)(m).

⁴² *Id.* §§ 153(1)(o); (q)

⁴³ *Id.* § 153(1)(p).

⁴⁴ *Id.* § 153(1)(z).

Australia has adopted procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons that Australia acquires under the Agreement. Article 7 of the Agreement requires Australia to adopt these procedures and sets forth restrictions that the procedures must contain, reflecting the targeting and minimization requirements set forth in 18 U.S.C. § 2523(b)(4) discussed below. The types of orders Australia may issue subject to the Agreement are discussed below. Australia's procedures incorporate the statutory restrictions in 18 U.S.C. §§ 2523(b)(2) and (b)(4), and the term "procedures" in the explanations below refers to the targeting and minimization procedures unless otherwise specified.

18 U.S.C. § 2523(b)(3) The terms of the Agreement do not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data.

The Agreement contains no language addressing whether providers must be capable of decrypting data, nor any limitation preventing providers from decrypting data, leaving those topics to be addressed, if at all, in domestic law or elsewhere.

18 U.S.C. § 2523(b)(4) The Agreement requires that, with respect to any order that is subject to the Agreement –

(A) Australia may not intentionally target a United States person or a person located in the United States, and has adopted targeting procedures designed to meet this requirement;

(B) Australia may not target a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States;

Australia's procedures contain targeting restrictions to minimize the acquisition of information concerning United States persons that Australia acquires under the Agreement. Consistent with 18 U.S.C. § 2523(b)(4)(A) and Article 4(3) of the Agreement, the procedures prohibit the intentional targeting of United States persons or persons located in the United States. Additionally, as required by 18 U.S.C. § 2523(b)(4)(B) and Article 4(4) of the Agreement, the procedures prohibit the targeting of a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States. In making these targeting assessments, the procedures require Australia to exercise reasonable due diligence by reviewing available sources of information to ensure that it is not targeting a United States person or person located in the United States.

(C) Australia may not issue an order at the request of or to obtain information to provide to the United States government or a third-party government, nor shall Australia be required to share any information produced with the United States government or a third-party government;

In accordance with 18 U.S.C. § 2523(b)(4)(C) and Article 5(4) of the Agreement, the procedures prohibit Australia from issuing an order on behalf of, or for the purpose of obtaining information to provide to, the United States government or a third-party government. Further, Article 9(3) of the Agreement prohibits Australia from being required to share any information produced with the United States government or a third-party government. In addition, the procedures include restrictions limiting Australia's sharing of data with the United States government.

(D) an order issued by Australia under the Agreement –

The orders Australia may issue under the Agreement satisfy 18 U.S.C. § 2523(b)(4)(D), which sets forth six procedural safeguards and other limitations. Australia will invoke the Agreement only with respect to orders authorized by the IPO Act. The following explains how each type of order Australia may issue under the Agreement and the IPO Act complies with each of the six requirements set out in Section 2523(b)(4)(D).

- (i) shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;

This requirement is set forth at Article 4(1) of the Agreement and is met through applicable Australian legislation and procedures. For instance, Parts 2 and 3 of the IPO Act authorize the issuance of certain orders for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of forms of serious crime which meet the definition under the Agreement of serious crime as an offense punishable by a maximum term of imprisonment of three years or more.⁴⁵ In addition, procedures implemented by Australian authorities mandate that all orders issued under this Agreement may only be issued for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of a serious crime, a requirement that will be confirmed by the Australian Designated Authority. The procedures also require Australia to record the specific offense for which each order was issued, enabling the United States later to confirm orders were issued consistent with this purpose requirement.

- (ii) shall identify a specific person, account, address, or personal device, or any other specific identifier as the object of the Order;

This requirement is set forth at Article 4(5) of the Agreement and is met through applicable Australian legislation and procedures. The IPO Act requires that international production orders obtainable under the Act target specific persons, accounts, addresses, or devices, by mandating, for example, that the order set out the specific “telecommunications identifiers” that would be subject to interception or seek the disclosure of stored communications related to an identified

⁴⁵ See IPO Act §§ 2 (defining “serious category 1 offense” and “serious category 2 offense”); see also §§ 30(2)(g) & (h); 39(2)(d); 48(2)(d); 60(2)(i) & (j); 69(2)(e); 78(2)(e).

“particular person.”⁴⁶ In addition, Australia has adopted targeting and minimization procedures that will require that Australia only issue international production orders against specific identifiers.

- (iii) shall be in compliance with the domestic law of Australia, and any obligation for a provider of an electronic communications service or a remote computing service to produce data shall derive solely from that law;

The first requirement is addressed by Article 5(1) of the Agreement, which requires that Australian orders subject to the Agreement shall be issued in compliance with Australian law, and by Article 5(7), which further requires that each Australian order subject to the Agreement must include a written certification by Australia’s Designated Authority that the Order is lawful and complies with the Agreement. The second requirement is addressed by Article 3(2) of the Agreement, which confirms that any legal effect of Australian orders derives solely from Australian law and that providers retain otherwise existing rights to raise applicable legal objections.

- (iv) shall be based on requirement for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation;

This requirement is set forth at Article 5(1) of the Agreement and is met through applicable Australian legislation and procedures.

The IPO Act requires that applications for orders sought in relation to violations of criminal law be accompanied by an affidavit which sets out the facts and other grounds on which the application is based.⁴⁷ For orders issued under Part 2, the issuing authority must be satisfied that the data sought in relation to the specified communications service would be likely to assist in the investigation of an identified serious crime in which a particular individual or telecommunications identifier is involved.⁴⁸ For orders issued under Part 3, the issuing authority must be satisfied that the data sought in relation to the specified communications service would be likely to substantially assist in: protecting the public from terrorist acts; preventing the provision of support for, or the facilitation of, a terrorist act; preventing the provision of support for, or the facilitation of, the engagement in hostile activity in a foreign country; or determining whether the control order has been or is being complied with.⁴⁹ The issuing authority must also take into account the gravity of the offense, any interference with privacy that would result from

⁴⁶ See *id.* §§ 2 (defining “telecommunication identifier”), 13 (describing how a “particular person may be identified”), 33 (requiring that a criminal IPO for stored communications must be “in respect of a particular person”); see also §§ 22, 31, 48, 61, 63, 72, 79, 90, 92, 101.

⁴⁷ *Id.* §§ 25, 36, 45, 55, 66, 75.

⁴⁸ *Id.* §§ 30(2)(g), 39(2)(d), 48(2)(d).

⁴⁹ *Id.* §§ 60(2)(i), 69(2)(e), 78(2)(e).

disclosing the data requested, alternative methods available to achieve the same ends, and any other matters the issuing authority considers relevant.⁵⁰

Orders relating to national security under the IPO Act must also be accompanied by an affidavit setting out the facts and other grounds on which the application is based.⁵¹ Where an order seeks communications, the Attorney-General must be satisfied that there are reasonable grounds for suspecting the services to which the order relates are being, or are likely to be, used for communications by an identified person engaged in, or likely to engage in, activities prejudicial to security and that the information likely to be obtained would be of national security use.⁵² The issuing authority must also be satisfied that there are reasonable grounds for suspecting that the services are being, or are likely to be, used for communications by an identified person engaged in, or likely to engage in, activities prejudicial to security, or, in some cases, be satisfied that the information likely to be obtained would likely be of use to ASIO in carrying out its intelligence collection functions.⁵³ Where an order seeks non-content data, the issuing authority must be satisfied that the data sought will be of use to ASIO in performing its functions.⁵⁴ Regardless of what data the order seeks in relation to national security, the issuing authority must take into account whether less intrusive, alternative methods are available to achieve the same ends and any other matters the issuing authority considers relevant.⁵⁵ The Australian Designated Authority shall not transmit an order relating to national security under the IPO Act pursuant to the Agreement unless the order is for the purpose of preventing, detecting, investigating, or prosecuting serious crime. In addition, ASIO is at all times subject to the Ministerial Guidelines issued by the Minister for Home Affairs to the Director-General of ASIO under the Australian Security Intelligence Organisation Act 1979 (“ASIO Act”).⁵⁶ The Guidelines set out matters that must be observed by ASIO in the performance of its functions and the exercise of its powers.

- (v) shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order;

This requirement is set forth at Article 5(2) of the Agreement and is met through applicable Australian legislation and procedures. IPOs may only be issued by certain judges, magistrates, or AAT members appointed by the Attorney-General to issue IPOs.⁵⁷ These are the same authorities that issue orders and warrants for the search of property in Australia and other purely domestic law enforcement actions. AAT members must also be enrolled legal practitioners of a

⁵⁰ *Id.* §§ 30(5)(a)(i)-(ix), 39(5)(a)(i)-(ix).

⁵¹ *Id.* §§ 86, 95, 104.

⁵² *Id.* §§ 83(6), 92(6),

⁵³ *Id.* §§ 89(2)(e)-(h).

⁵⁴ *Id.* §§ 107(2)(d).

⁵⁵ *Id.* §§ 89(5)(a)-(b), 98(3)(a)-(d), 107(5)(a)-(d).

⁵⁶ See Ministerial Guidelines, available at

<https://www.asio.gov.au/sites/default/files/Minister's%20Guidelines%20to%20the%20Australian%20Security%20Intelligence%20Organisation.pdf>.

⁵⁷ See IPO Act §§ 14, 15, 16, 17.

federal court or of the Supreme Court of a state or territory for at least five years.⁵⁸ IPOs relating to national security must be issued by an AAT member who is a Deputy President or member of the Security Division of the Administrative Appeals Tribunal.⁵⁹

These officials are insulated from political influence as the IPO Act provides issuing authorities with the same protection and immunity in relation to their performance or exercise of a function under the Act as is conferred upon a Justice of the High Court in relation to proceedings in the High Court.⁶⁰ Judges of Commonwealth courts may not be removed except by request by both Houses of Parliament on the grounds of proved misbehavior or incapacity.⁶¹ AAT members are appointed to their positions for an established term not to exceed seven years, subject to renewal.⁶² AAT members may not be removed except by request by both Houses of Parliament on the grounds of proved misbehavior or incapacity or by the Governor-General for excessive absence from duty, financial insolvency, unauthorized outside employment, or undisclosed conflicts of interest.⁶³

- (vi) in the case of an order for the interception of wire or electronic communications, and any extensions thereof, shall require that the interception order: (I) be for a fixed, limited duration; (II) may not last longer than is reasonably necessary to accomplish the approved purposes of the order; and (III) be issued only if the same information could not reasonably be obtained by another less intrusive method;

This requirement is set forth at Article 5(3) of the Agreement, and orders subject to the Agreement for the interception of communications that are issued under the IPO Act must comply with these requirements based on provisions set forth in the Australian targeting and minimization procedures. In addition, the IPO Act sets maximum time limits for interception orders.⁶⁴ Further, the Ministerial Guidelines require that covered investigatory activities seek to minimize the intrusion on the privacy of affected individuals, including by using the least intrusive method where possible.⁶⁵

(E) an order issued by Australia may not be used to infringe freedom of speech;

The Agreement requires in Article 4(2) that orders subject to the Agreement may not be used to infringe freedom of speech. In further implementation of this requirement, Article 9(4) provides

⁵⁸ *Id.* §§ 15, 16.

⁵⁹ *Id.* § 17.

⁶⁰ *Id.* §§ 14, 15, 16, 17.

⁶¹ Commonwealth of Australia Constitution Act § 72.

⁶² Administrative Appeals Tribunal Act 1975 § 8.

⁶³ *Id.* § 13.

⁶⁴ IPO Act § 30(4), 60(4), 89(4).

⁶⁵ Ministerial Guidelines at § 3.4.

that where Australia has received data in response to an order subject to the Agreement and 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, then Australia must obtain permission from the United States prior to use of the data in a manner that is or could be contrary to those essential interests. The United States has so declared, in a letter signed contemporaneously with the Agreement, that its essential interests relating to freedom of speech concerns may be so implicated. The letter also specifies certain Australian categories of offenses that may raise freedom of speech concerns, describes other circumstances under which such concerns may arise, and provides that the United States may unilaterally supplement that list of categories.

(F) Australia shall promptly review material collected pursuant to the Agreement and store any unreviewed communications on a secure system accessible only to those persons trained in applicable procedures;

The procedures require that all unreviewed data be retained in a secure system that is only accessible to those personnel trained in the procedures, in accordance with 18 U.S.C. § 2523(b)(4)(F) and Article 7(4) of the Agreement. Moreover, the procedures require Australia to confirm, after electronic data is collected, that its initial targeting assessment was correct by promptly reviewing an appropriate sample of the collection in accordance with 18 U.S.C. § 2523(b)(4)(F).

(G) Australia shall, using procedures that, to the maximum extent possible, meet the definition of minimization procedures in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801), segregate, seal, or delete, and not disseminate material found not to be information that is, or is necessary to understand or to assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or serious bodily harm to any person;

The procedures contain provisions to minimize the retention and dissemination of information of or concerning United States persons that Australia acquires under the Agreement. For example, consistent with 18 U.S.C. § 2523(b)(4)(G) and Article 7(3) of the Agreement, the procedures require that United States person information that is determined 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 serious crime, or necessary to protect against a threat of death or serious bodily harm to any person, shall be destroyed and not disseminated. In addition, the procedures mandate that communications of or concerning United States persons should be masked or redacted, except in narrow circumstances where: (1) the United States person has consented to the dissemination; (2) the information of or concerning the United States person is publicly available; or (3) the United States person information meets the dissemination standard set forth in 18 U.S.C. § 2523(b)(4)(G). Further, the procedures set forth retention time periods for unminimized information acquired pursuant to the Agreement. Finally,

to further minimize the retention of United States person information, the procedures prohibit the querying of known identifiers of United States persons in the unminimized content of communications acquired pursuant to the Agreement, except for the narrow purpose of identifying data that should be destroyed for compliance reasons in accordance with the procedures.

(H) Australia may not disseminate the content of a communication of a United States person to United States authorities unless the communication may be disseminated pursuant to subparagraph (G) and relates to significant harm, or the threat thereof, to the United States or United States persons, including crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud;

Consistent with 18 U.S.C. § 2523(b)(4)(H) and Article 7(5) of the Agreement, the procedures prohibit Australia from disseminating to United States authorities the content of a communication of a United States person that Australia acquires under the Agreement, unless the communication can be disseminated pursuant to the standard described above in 18 U.S.C. § 2523(b)(4)(G) and the communication relates to a significant harm, or the threat thereof, to the United States or United States persons, including crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud. Moreover, the procedures further protect such United States person information by requiring that any dissemination of the content of a communication of a United States person to United States authorities be accompanied by a cover note informing the authority of its obligation to comply with 18 U.S.C. § 2523(h) to use minimization procedures to appropriately protect non-publicly available information concerning United States persons and advising it to consult with the Department of Justice.

(I) Australia shall afford reciprocal rights of data access, to include, where applicable, removing restrictions on communications service providers, including providers subject to United States jurisdiction, and thereby allow them to respond to valid legal process sought by a governmental entity if Australian laws would otherwise prohibit communications service providers from disclosing the data;

Article 3(1) of the Agreement provides that Australia undertakes to ensure that its domestic laws relating to the preservation, authentication, disclosure, and production of electronic data will permit providers to comply with United States orders subject to the Agreement. The Agreement's entry into force will serve to remove such restrictions currently in place under Australian law, for example through IPO Act provisions permitting providers to disclose data in response to a data request made under a designated international agreement.⁶⁶

⁶⁶ IPO Act. §§ 168, 169.

(J) Australia shall agree to periodic review of its compliance with the terms of the Agreement to be conducted by the United States government.

The procedures incorporate auditing and reporting requirements consistent with 18 U.S.C. § 2523(b)(4)(J) and Article 11(1) of the Agreement. The Department of Justice will conduct periodic reviews of Australia's compliance with the terms of the Agreement and the targeting and minimization procedures. To support these compliance reviews, in the first instance, the procedures require Australian agencies that request orders subject to the Agreement to record and report certain breaches or instances of noncompliance with the procedures and the Agreement. Australia will then report instances of noncompliance to the Department of Justice. The procedures also require Australia's Attorney-General's Department to conduct periodic audits of Australia's compliance with the procedures and Agreement. Instances of noncompliance discovered through those audits will be reported to the Department of Justice. The Department of Justice will gather additional information, as necessary, regarding the instances of noncompliance, including the causes of such compliance issues and actions taken by Australia to remedy them. In addition, through reviewing the information provided by Australia regarding instances of noncompliance, the Department of Justice will look to identify trends in compliance issues and determine through discussions with Australia whether additional remedial actions may be taken to prevent such issues from occurring.

(K) the United States Government has reserved the right to render the Agreement inapplicable as to any order for which the United States Government concludes the Agreement may not be properly invoked;

Article 5(12) of the Agreement provides that if the United States concludes that Australia has not properly invoked the Agreement with respect to any order, it shall notify Australia and the relevant provider of that conclusion, and the Agreement shall not apply to that order. This right of the United States to render the Agreement inapplicable to a specific order could arise in the context of the dispute resolution mechanism envisaged in Article 5(11) of the Agreement, if a provider raises specific objections about an order, or in any other circumstance.