**U.S. Department of Justice**

Office of Legislative Affairs

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

DEC 04 2019

The Honorable Lindsey Graham
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable Jim Risch
Chairman
Committee on Foreign Relations
United States Senate
Washington, DC 20510

The Honorable Dianne Feinstein
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable Bob Menendez
Ranking Member
Committee on Foreign Relations
United States Senate
Washington, DC 20510

Dear Chairmen and Ranking Members:

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 and the Senate Foreign Relations Committee:

- Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, 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 may provide additional assistance regarding this or any other matter.

Sincerely,

Stephen E. Boyd
Assistant Attorney General

Enclosures

**Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime**

The Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland (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 respecting privacy, human rights, and civil liberties, including freedom of speech, and due process of law;

Intending to provide standards of protection that comply with the Parties' respective laws for the treatment of electronic data containing personal data, and to create a legally binding and enforceable instrument between public authorities that provides appropriate safeguards for that purpose;

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 necessity and proportionality or probable cause and limitations on overbreadth of orders, and independent judicial 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. Computer System has the meaning set forth in Chapter I Article 1a of the Budapest Convention on Cybercrime, to wit: any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.
3. 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.
4. Covered Information means Covered Data for Accounts used or controlled by a Covered Person and not also used or controlled by any Receiving-Party Person.
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 subsection (i).

8. Designated Authority means the governmental entity designated, for the United Kingdom, by the Secretary of State for the Home Department, and for the United States, by the Attorney General.

9. Issuing Party means the Party that issues the relevant Legal Process. Where the United States is the Issuing Party, this includes where Legal Process is issued by state, local, territorial, tribal, or any other authorities within the United States. Where the United Kingdom is the Issuing Party, this includes where Legal Process is issued by authorities of the state within the United Kingdom of Great Britain and Northern Ireland.

10. Legal Process means Orders subject to this Agreement as well as preservation process and Subscriber Information process recognized by Article 10 of this Agreement.

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, whether for stored or live communications.

12. Receiving-Party Person means:

    Where the United States is the Receiving Party:

    (i) any governmental entity or authority thereof, including at the state, local, territorial, or tribal level;

    (ii) a citizen or national thereof;

    (iii) a person lawfully admitted for permanent residence;

    (iv) an unincorporated association a substantial number of members of which fall into subsections (ii) or (iii);

    (v) a corporation that is incorporated in the United States; or

    (vi) a person located in its territory; and

    Where the United Kingdom is the Receiving Party:

    (i) any governmental entity or authority of the state;

    (ii) an unincorporated association, a substantial number of members of which are located in its territory;

    (iii) a corporation located or registered in its territory; or

    (iv) any other person located in its territory.

13. Receiving Party means the Party, including political subdivisions thereof, other than the Issuing Party.

14. Serious Crime means an offense that is punishable by a maximum term of imprisonment of at least three years.

15. 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.

16. U.S. Person means:

    (i) a citizen or national of the United States;

    (ii) a person lawfully admitted for permanent residence;

    (iii) an unincorporated association a substantial number of members of which fall into subsections (i) or (ii); or

    (iv) a corporation that is incorporated in the United States.

**Article 2: Purpose of the Agreement**

1. The purpose of this Agreement is to advance public safety and security, and to protect privacy, 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. The Agreement provides an efficient, effective, data protection-compatible and privacy-protective means for each Party to obtain, subject to appropriate targeting limitations, electronic data relating to the prevention, detection, investigation, or prosecution of Serious Crime, in a manner consistent with its law and the law of the other Party.

2. Without prejudice to the applicability of any other legal basis or other important interests under the respective Parties' laws, this Agreement supports:

    a. the judicial activities of courts, as well as the legal obligations and claims under the respective Parties' laws;

    b. substantial public interests of both Parties, and the tasks necessary to accomplish those interests; and

    c. legitimate interests properly and appropriately pursued.

3. Interests relevant to this Agreement include, but are not limited to:

    a. the prevention, detection, investigation, or prosecution of Serious Crime by each Party, whether or not the crimes are transnational in nature or impact. Such matters being in the interests of both Parties given their commitment to the Rule of Law and justice being served as well as in recognition of the practical reality that Serious Crime can have direct or indirect effects outside the border of the Issuing Party;

    b. the spirit of reciprocity in international cooperation, whereby the interest of each Party in being able to obtain electronic data pursuant to this Agreement requires them to provide the same ability to the other Party to obtain such information in the opposite direction on a reciprocal basis;

    c. the furthering of international cooperation in order to counter and discourage the exploitation of data localization by criminals seeking to shield themselves from scrutiny by choice of jurisdiction;

    d. the establishment of a system of access to electronic data that is comprehensively governed by binding, appropriate and substantial safeguards for protecting the civil liberties and rights of individuals incorporating, as applicable under the Parties' respective legal systems, standards such as probable cause, necessity and proportionality, independent

judicial oversight, and the requirements of laws relating to the handling and processing of data relating to individuals.

**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 Orders subject to this Agreement. 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 shall apply to an Order as to which the Issuing Party invokes this Agreement, with notice to the relevant Covered Provider. Any legal effect of an Order subject to this Agreement derives solely from the law of the Issuing Party. Covered Providers retain otherwise existing rights to raise applicable legal objections to an Order subject to this Agreement.
3. Each Party in executing this Agreement recognizes that the domestic law of the other Party, 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 subject to this Agreement. Each Party shall advise the other of any material changes in its domestic law that significantly affect the protections for Covered Data and shall consult regarding any issues arising under this paragraph pursuant to Article 5 or Article 11.
4. This Agreement is intended to facilitate the ability of the Parties to obtain 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 fully implemented, including the provisions of Article 9, consistent with the constitutional structure and principles of each Party.

**Article 4: Targeting Restrictions**

1. Orders subject to this Agreement must 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 may 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 may 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 may not target a Covered Person if the purpose is to obtain information concerning a Receiving-Party Person.
5. Orders subject to this Agreement must be targeted at specific Accounts and shall identify as the object of the Order a specific person, account, address, or personal device, or any 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; may 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 may 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. Such Orders shall be transmitted by the Issuing Party's Designated Authority. The Designated Authorities of the Parties may mutually agree 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 in whole or in part. The Designated Authorities of the Parties may, by mutual agreement, 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 the Order.

9. The Issuing Party's Designated Authority 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 the Issuing Party and is not a national 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 notification would be detrimental to operational or national security, 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 the Order. Upon receipt of objections to an 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, 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 Information 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 Information 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 legal obligation Covered Providers have to produce data in response to Legal Process issued pursuant to the law of the Issuing Party.
4. The Issuing Party's requirements as to the manner in which Covered Information is produced 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.

**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. The United Kingdom shall adopt and implement appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning U.S. Persons acquired pursuant to an Order subject to this Agreement, consistent with the need of the United Kingdom to acquire, retain, and disseminate Covered Information 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 the United Kingdom 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 or physical harm to any person.
4. The minimization procedures shall include rules requiring the United Kingdom 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 the United Kingdom may 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: Limitations on Use and Transfer**

1. Without prejudice to limitations specified elsewhere in this Agreement, data acquired by the Issuing Party pursuant to an Order subject to this Agreement 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 country 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 an Order subject to this Agreement 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. the United Kingdom 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 the United Kingdom 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's Designated Authority 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 9: Privacy and Data Protection Safeguards**

1. The Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses done at Amsterdam, 2 June 2016, shall be applied mutatis mutandis by the Parties to all personal information produced in the execution of Orders subject to this Agreement to provide equivalent protections. For the United States, the principal laws implementing Article 19 of that agreement in this context are the Judicial Redress Act of 2015 and the Freedom of Information Act.

2. The processing and transfer of data in the execution of Orders subject to this Agreement are compatible with the Parties' respective applicable laws regarding privacy and data protection.

**Article 10: Preservation Process and Subscriber Information**

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 under the domestic law of the Issuing Party that regards:

a. the preservation of Covered Data or Subscriber Information, or

b. the disclosure, production, or authentication of Subscriber Information

relating to the prevention, detection, investigation, or prosecution of crime.

2. The Issuing Party may issue such process directly to a Covered Provider. Such process shall be issued in compliance with and subject to review or oversight under the domestic law of the Issuing Party. Any legal effect of such process derives solely from the law of the Issuing Party. Covered Providers retain otherwise existing rights to raise applicable legal objections.

3. Such process shall be reasonable and must be issued for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of crime.

4. Such process may 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.

5. Subscriber Information acquired pursuant to such process shall be treated in accordance with the domestic law of the Issuing Party, including its privacy and freedom of information laws, as well as the applicable provisions of the Agreement.

6. An Issuing Party and a Covered Provider may make arrangements for the secure transmission of such process and Subscriber Information produced in response, consistent with applicable law.

7. The Issuing Party shall not be required to share any Subscriber Information with the Receiving Party or a third-party government.

8. Each Party shall advise the other of any material changes in its domestic law that significantly affect the protections for preserved Covered Data or Subscriber Information, or would substantially frustrate or impair the operation of such process, and shall consult regarding any issues arising under this paragraph.

9. The Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses done at Amsterdam, 2 June 2016, shall be applied mutatis mutandis by the Parties to all personal information preserved or Subscriber Information produced pursuant to such process. For the United States, the principal laws implementing Article 19 of that agreement in this context are the Judicial Redress Act of 2015 and the Freedom of Information Act.

10. In light of the safeguards recognized in this Article and the domestic law of each party including the implementation of that law, there are robust substantive and procedural protections for privacy and civil liberties in relation to such process. The processing and transferring of data pursuant to such process is compatible with the Parties' respective applicable laws regarding privacy and data protection.

11. The Issuing Party's requirements as to the manner in which Subscriber Information is produced 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.

**Article 11: Compatibility and Non-Exclusivity**

1. This 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 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.

2. This Agreement shall constitute, with respect to the compulsory measures arising from Orders subject to this Agreement and such process for preservation and Subscriber Information recognized in Article 10, the consultation, exhaustion, and other requirements of paragraphs 2, 3, 4, 5, and 6 of Article 18 of the Annex to the Instrument as contemplated by Article 3(2) of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003, as to the application of the Treaty between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Mutual Legal Assistance in Criminal Matters signed at Washington 6 January 1994, signed at London 16 December 2004.

**Article 12: Review of Implementation and Consultations**

1. Within one year of this Agreement's entry into force, and periodically thereafter, 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 Orders subject to this Agreement to determine whether to modify procedures adopted under this Agreement.

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

3. In the event that the Parties are unable to resolve a concern about the implementation of this Agreement or a dispute, either Party may conclude that the Agreement may not be invoked with respect to an identified category of Legal Process, including Legal Process that are issued on or after a particular date. Notification of that conclusion must be sent by the Designated Authority of the Party that has so concluded to the Designated Authority of the other Party. The notified Party shall not invoke the Agreement with respect to any Legal Process within the identified category upon receipt of such notification. Such a conclusion may be revoked at any time, in whole or in part, by the Party that reached the conclusion through a notification of the revocation to the other Party's Designated Authority. Any data produced to the Issuing Party shall continue to be subject to the conditions and safeguards, including minimization procedures, set forth in this Agreement.

4. 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.

5. 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 13: Costs**

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

**Article 14: Amendments**

This Agreement may be amended by written agreement of the Parties at any time.

**Article 15: Temporal Application**

This Agreement shall apply to Legal Process issued by an Issuing Party on or after the Agreement's entry into force.

**Article 16: 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 17: Expiry and Termination of the Agreement**

1. This Agreement shall remain in force for a five year period unless, prior to the expiry of the Agreement, the Parties agree in writing, through an exchange of diplomatic notes, to extend the Agreement for a further five years (or any other period as may be agreed between them).
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, 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 3rd day of October, 2019, in duplicate, in the English language.

FOR THE GOVERNMENT OF THE UNITED STATES OF AMERICA:

FOR THE GOVERNMENT OF THE UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND:

3 October 2019

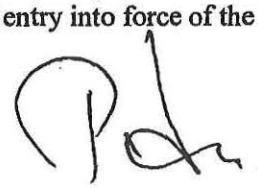
Dear Attorney General Barr,

I have the honour to refer to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland 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 8(4) of the Agreement be interpreted and applied as per the following understandings.

The United Kingdom declares that its essential interests under the Agreement may be implicated by the introduction of data received pursuant to Legal Process recognised 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 the United Kingdom prior to any use of the data in a manner that is or could be contrary to those essential interests, as described in Article 8(4).

If the foregoing 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,



The Rt. Hon. Priti Patel MP, Secretary of State for the Home Department.

October 3, 2019

Dear Home Secretary Patel,

I have the honor to refer to your letter dated October 3, 2019, regarding the Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland 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 the United Kingdom of Great Britain and Northern Ireland 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 8(4) of the Agreement be interpreted and applied as per the following understandings.*
>
> *The United Kingdom declares that its essential interests under the Agreement may be implicated by the introduction of data received pursuant to Legal Process recognised 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 the United Kingdom prior to any use of the data in a manner that is or could be contrary to those essential interests, as described in Article 8(4).*
>
> *If the foregoing 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,

WPBarr

William P. Barr, Attorney General of the United States of America.

3 October 2019

Dear Attorney General Barr,

I have the honour to refer to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland 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 10 of the Agreement be applied as per the following understandings.

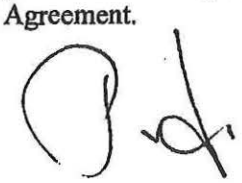
The issuance of Legal Process, as recognised in Article 10 of the Agreement, by an Issuing Party conforms with the relevant requirements of the Convention on Cybercrime, done at Budapest November 23, 2001, including the principle of proportionality and other conditions and safeguards as set forth in article 15.

Where the Issuing Party is the United States, preservation process is issued pursuant to Title 18, United States Code, Section 2703(f), which is the domestic law that grants the government authority to request preservation of data by electronic communication service providers and remote computing service providers. Section 2703(f) directs providers to preserve data upon request for an initial period of 90 days, which time period can be extended once for an additional 90 days. Where the Issuing Party is the United Kingdom, preservation process is issued pursuant to the relevant common law. For the purposes of Article 10 of the Agreement, the United Kingdom intends to limit such preservation to an initial period of 90 days that can be extended once for up to an additional 90 days.

Where the Issuing Party is the United States, all Legal Process for Subscriber Information, as recognised in Article 10 of the Agreement, has a domestic legal basis in Title 18, United States Code, Sections 2703 or 2709, which are the domestic laws that permit governmental entities to obtain legal process seeking to compel disclosure of such information by electronic communication service providers and remote computing service providers. This Legal Process is subject to all rights and protections granted by the Constitution, legal precedent, and the relevant domestic Rules of Criminal Procedure, including the ability to quash such a process where it is unreasonable. Where the United Kingdom is the Issuing Authority, all Legal Process for Subscriber Information, as recognised in Article 10 of the Agreement, has a domestic legal basis in the Investigatory Powers Act 2016, the Regulation of Investigatory Powers Act 2000, and Judicial Orders, which are the domestic laws or mechanisms pursuant to which a UK authority may compel disclosure of communications data by a telecommunications provider.

If the foregoing 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 application of the Agreement, which would be operative on the date of entry into force of the Agreement.

Sincerely,



The Rt. Hon. Priti Patel MP, Secretary of State for the Home Department.

October 3, 2019

Dear Home Secretary Patel,

I have the honor to refer to your letter dated October 3, 2019, regarding the Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland 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 the United Kingdom of Great Britain and Northern Ireland 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 10 of the Agreement be applied as per the following understandings.*

*The issuance of Legal Process, as recognised in Article 10 of the Agreement, by an Issuing Party conforms with the relevant requirements of the Convention on Cybercrime, done at Budapest November 23, 2001, including the principle of proportionality and other conditions and safeguards as set forth in article 15.*

*Where the Issuing Party is the United States, preservation process is issued pursuant to Title 18, United States Code, Section 2703(f), which is the domestic law that grants the government authority to request preservation of data by electronic communication service providers and remote computing service providers. Section 2703(f) directs providers to preserve data upon request for an initial period of 90 days, which time period can be extended once for an additional 90 days. Where the Issuing Party is the United Kingdom, preservation process is issued pursuant to the relevant common law. For the purposes of Article 10 of the Agreement, the United Kingdom intends to limit such preservation to an initial period of 90 days that can be extended once for up to an additional 90 days.*

*Where the Issuing Party is the United States, all Legal Process for Subscriber Information, as recognised in Article 10 of the Agreement, has a domestic legal basis in Title 18, United States Code, Sections 2703 or 2709, which are the domestic laws that permit governmental entities to obtain legal process seeking to compel disclosure of such information by electronic communication service providers and remote computing service providers. This Legal Process is subject to all rights and protections granted by the Constitution, legal precedent, and the relevant domestic Rules of Criminal Procedure, including the ability to quash such a process where it is unreasonable. Where the United Kingdom is the Issuing Authority, all Legal Process for Subscriber Information, as recognised in Article 10 of the Agreement, has a domestic legal basis in the Investigatory Powers Act 2016, the Regulation of Investigatory Powers Act 2000, and Judicial Orders, which are the domestic laws or mechanisms pursuant to which a UK authority may compel disclosure of communications data by a telecommunications provider.*

*If the foregoing 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 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 application of the Agreement, which would be operative on the date of entry into force of the Agreement.

Sincerely,

WPBarr

William P. Barr, Attorney General of the United States of America.

October 3, 2019

Dear Home Secretary Patel,

I have the honor to refer to the Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime (the "Agreement"), signed today, and to propose that the Agreement be applied as per the following understanding.

The United States commits to inform the United Kingdom 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 the United Kingdom if the Department of Defense intends to use data known by relevant Department personnel to have been obtained pursuant to Legal Process recognized 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 the Government of the United Kingdom of Great Britain and Northern Ireland, 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,

WPBarr

William P. Barr, Attorney General of the United States of America.

3 October 2019

Dear Attorney General Barr,

I have the honour to refer to your letter dated 3 October 2019, regarding the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland 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 the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), signed today, and to propose that the Agreement be applied as per the following understanding.*
>
> *The United States commits to inform the United Kingdom 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 the United Kingdom if the Department of Defense intends to use data known by relevant Department personnel to have been obtained pursuant to Legal Process recognized 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 the Government of the United Kingdom of Great Britain and Northern Ireland, 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 the United Kingdom of Great Britain and Northern Ireland, I am pleased to convey that your proposal is acceptable. Your letter and this reply constitute an understanding of our two Governments in this matter as to the application of the Agreement, which would be operative on the date of entry into force of the Agreement.

Sincerely,

The Rt. Hon. Priti Patel MP, Secretary of State for the Home Department.

October 3, 2019

Dear Home Secretary Patel,

I have the honor to refer to the Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), signed today, and to propose that Article 8(4) of the Agreement be interpreted and applied as per 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 recognized by the Agreement as evidence in the prosecution's case in the United Kingdom in a manner that raises freedom of speech concerns for the United States. Accordingly, in the event that authorities in the United Kingdom 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, as further described in this letter, the Designated Authority of the United Kingdom 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 8(4).

The United States declares that the introduction of data received pursuant to Legal Process recognized by the Agreement as evidence in a UK prosecution under the following statutes may raise freedom of speech concerns for the United States, depending on the facts, such that consultation with and obtaining permission from the Designated Authority of the United States is appropriate prior to any such use of the data:

- Terrorism Act 2006 c.11, s.1 and 2, including how those provisions are to be applied to internet activity as set out in s.3
- Terrorism Act 2000 c.11, s.12(1A) and 13
- Terrorism Act 2000 c.11, s.58(1) and 58A(1)
- Public Order Act 1986 c.64, s.18-23, s.29B-29G
- Official Secrets Act 1989 c.6, s.5, in the context of activities that are journalistic in nature
- Communications Act 2003 c.21, s.127
- Protection from Harassment Act 1997 c.40, s.2 and 2A, in the context of both the making or publishing of statements that may be viewed as harassing

In addition to offenses under the listed statutes, there could be prosecutions for other offenses that may raise freedom of speech concerns for the United States, depending on the facts, such as those involving news gathering and publication, or public protest. When UK officials intend to use such data in a UK prosecution of any other offense under a statute not listed above, but have reason to believe, based on the context of the case and their understanding of U.S. views, including the United Kingdom's experience under the Mutual Legal Assistance process, that the introduction of the data as evidence in the prosecution's case might raise freedom of speech concerns for the United States, the Designated Authority of the United Kingdom should

consult with the Designated Authority of the United States. If the Designated Authority of the United States confirms that there are freedom of speech concerns, such data should not be introduced in the prosecution's case without permission as set forth in Article 8(4).

Finally, the United States may unilaterally supplement the list of statutes set forth above should other UK statutes, either applied currently or 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 the United Kingdom 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,

WPBarr

William P. Barr, Attorney General of the United States of America.

3 October 2019

Dear Attorney General Barr,

I have the honour to refer to your letter dated 3 October 2019 regarding the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland 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 the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), signed today, and to propose that Article 8(4) of the Agreement be interpreted and applied as per 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 recognized by the Agreement as evidence in the prosecution's case in the United Kingdom in a manner that raises freedom of speech concerns for the United States. Accordingly, in the event that authorities in the United Kingdom 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, as further described in this letter, the Designated Authority of the United Kingdom 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 8(4).*

*The United States declares that the introduction of data received pursuant to Legal Process recognized by the Agreement as evidence in a UK prosecution under the following statutes may raise freedom of speech concerns for the United States, depending on the facts, such that consultation with and obtaining permission from the Designated Authority of the United States is appropriate prior to any such use of the data:*

- *Terrorism Act 2006 c.11, s.1 and 2, including how those provisions are to be applied to internet activity as set out in s.3*
- *Terrorism Act 2000 c.11, s.12(1A) and 13*
- *Terrorism Act 2000 c.11, s.58(1) and 58A(1)*
- *Public Order Act 1986 c.64, s.18-23, s.29B-29G*
- *Official Secrets Act 1989 c.6, s.5, in the context of activities that are journalistic in nature*
- *Communications Act 2003 c.21, s.127*
- *Protection from Harassment Act 1997 c.40, s.2 and 2A, in the context of both the making or publishing of statements that may be viewed as harassing*

*In addition to offenses under the listed statutes, there could be prosecutions for other offenses that may raise freedom of speech concerns for the United States, depending on the facts, such as those involving news gathering and publication, or public*

*protest. When UK officials intend to use such data in a UK prosecution of any other offense under a statute not listed above, but have reason to believe, based on the context of the case and their understanding of U.S. views, including the United Kingdom's experience under the Mutual Legal Assistance process, that the introduction of the data as evidence in the prosecution's case might raise freedom of speech concerns for the United States, the Designated Authority of the United Kingdom should consult with the Designated Authority of the United States. If the Designated Authority of the United States confirms that there are freedom of speech concerns, such data should not be introduced in the prosecution's case without permission as set forth in Article 8(4).*

*Finally, the United States may unilaterally supplement the list of statutes set forth above should other UK statutes, either applied currently or 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 the United Kingdom 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 the United Kingdom of Great Britain and Northern Ireland, 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,

The Rt. Hon. Priti Patel MP, Secretary of State for the Home Department.

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

November 27, 2019

Dear Home Secretary Patel:

I have the honor to refer to the Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime ("the Agreement"), signed October 3, 2019, and the letter ("the Freedom of Speech Letter") signed and exchanged October 3, 2019, regarding the interpretation and application of Article 8(4) of the Agreement with regard to the essential interests of the United States.

The United States hereby supplements the list of statutes set forth in the Freedom of Speech Letter by adding the following:

- Malicious Communications Act 1988 c.27, s.1
- Malicious Communications (Northern Ireland) Order 1988 No. 1849 (N.I. 18), Art. 3

In addition, any relevant legal authorities establishing Scottish or Northern Ireland offenses analogous to the offenses established by the authorities listed in the Freedom of Speech Letter, as supplemented, should be treated as though they have been included in the list.

This supplement to the Freedom of Speech Letter is intended to become effective on the same date the Freedom of Speech Letter becomes operative.

Sincerely,

William P. Barr
Attorney General

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

November 27, 2019

On October 3, 2019, the Home Secretary of the United Kingdom and I signed the Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland 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 United States 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. Secretary of State Pompeo has concurred with this determination.

Sincerely,

William P. Barr
Attorney General

# 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 the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, signed at Washington, D.C., on October 3, 2019 ("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 with respect to these considerations 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 the United Kingdom of Great Britain and Northern Ireland ("United Kingdom" or "UK"), 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 the United Kingdom 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 UK-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 2018 Country Report on Human Rights Practices in the United Kingdom (the "UK Country Report"). Consultations and information reviewed indicate that the United Kingdom 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**

The United Kingdom 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. The United Kingdom 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

[1] Experts and civil society organizations provided comments directly to the Department of Justice and the Department of State. These organizations raised a range of concerns about, *inter alia*, the scope or implementation of UK criminal and national security legislation, including: the Anti-Social Behavior, Crime and Policing Act 2014; the Justice and Security Act 2013; UK Online Harms Paper; the Terrorism Act 2006; the Public Order Act 1986; the Committee Against Torture; the Crime (Overseas Production Orders) Act 2019; and the Investigatory Powers Act 2016. These concerns were taken into consideration, as appropriate, but did not undercut the conclusions reached for the purposes of the determination and certification.

against Torture. The United Kingdom has adopted legislation and policies to give effect to its obligations under these treaties.

The United Kingdom incorporated the European Convention on Human Rights (ECHR) into its domestic law through the adoption of the Human Rights Act 1998 (HRA). Under the HRA, which came into force in October 2000, rights set out in the ECHR are enforceable in United Kingdom courts. Every United Kingdom resident – regardless of nationality – may seek the enforcement of those rights, and public authorities have a legal obligation to respect them. Moreover, the HRA empowers the judiciary to issue a Declaration of Incompatibility, which is a statement that a law is incompatible with human rights and must be changed. All UK legislation is required to be compatible with the rights set out in the ECHR.

The United Kingdom 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 other human rights-related processes mechanisms, including United Nations Special Procedures.

**18 U.S.C. § 2523(b)(1)(B)(i)** **The United Kingdom 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.**

The United Kingdom is a party to the Convention on Cybercrime, done at Budapest on November 23, 2001 (the "Budapest Convention"). The United Kingdom was already largely compliant with the Budapest Convention at the time of signature of the Convention, but a number of legislative and non-legislative changes were required before ratification. Amendments to the Computer Misuse Act 1990 were made in the Police & Justice Act 2006 and the Serious Crime Act 2007 to ensure full compliance. These came into force in October 2008. The United Kingdom then ratified the Budapest Convention on May 25, 2011, with an entry into force on September 1, 2011.

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

The United Kingdom has demonstrated and continues to demonstrate respect for the rule of law and principles of non-discrimination. In the United Kingdom the rule of law is recognized as a constitutional principle derived from common law and is given effect by an independent and impartial judiciary. The United Kingdom's respect for principles of non-discrimination, in particular, is demonstrated by its becoming party to, inter alia, the ECHR, which prohibits discrimination and which is incorporated into United Kingdom domestic law through the HRA. Many UK laws implement these principles of non-discrimination, including the Equality Act 2006 and Equality Act 2010. The Equality Act 2006 also established the UK Equality and Human Rights Commission, which serves as a regulatory body.

According to the UK Country Report:

> [T]he law provides the same legal status and rights for women and men. Women were subject to some discrimination in employment. [...] The law prohibits discrimination against persons with physical, sensory, intellectual, and mental disabilities. The government effectively enforced the law. [...] The law prohibits racial and ethnic discrimination, but Travellers, Roma, and persons of African, Afro-Caribbean, South Asian, and Middle Eastern origin at times reported mistreatment on racial or ethnic grounds. [...] The law in England and Wales prohibits discrimination and harassment based on sexual orientation. [...] The law prohibits discrimination in employment or occupation regarding race, color, sex, religion or belief, political opinion, national origin or citizenship, social origin, disability, sexual orientation, gender identity or reassignment, marriage and civil partnership, being pregnant or on maternity leave, age, language, or HIV or other communicable disease status. [...] The government effectively enforced these laws and regulations.

**18 U.S.C. § 2523(b)(1)(B)(iii) The United Kingdom 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.

According to the UK Country Report, UK law prohibits arbitrary or unlawful interference with privacy, family, the home, or correspondence. The United Kingdom has multiple governmental bodies charged with overseeing and enforcing these laws, including the UK Information Commissioner, who conducts frequent investigations into alleged violations of privacy rights, and generally makes her reports public. Finally, UK courts have long been available for redress to individuals who can establish violations of their rights. Article 8 of the ECHR, as incorporated into UK domestic law through the HRA, governing the right to privacy, states:

> Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Under the HRA, the right to privacy is thus subject to restrictions only when "necessary" for the purposes specified in the law, including for national security, public safety, crime prevention, and the protection of the rights and freedoms of others.

The Investigatory Powers Act 2016 c. 25 (IPA) sets out the circumstances under which certain investigatory powers are necessary and appropriate despite the privacy interests of an individual

and covers interception, equipment interference, and acquisition of communications data, among other areas. Metadata retention provisions under the IPA allow the Secretary of State for the Home Department to issue notices requiring telecommunications providers to capture information metadata about user activity, including the acquisition and retention of internet connection records, and retain it for up to 12 months. The IPA authorizes warrants under a variety of circumstances and for various purposes. These include warrants for targeted interception of content and non-content communications data, as well as bulk interception and bulk acquisition of communications data sent or received by individuals outside the British Isles, and bulk equipment interference involving "overseas-related" communications, information, and equipment data. In April 2018, the UK High Court ruled that part of the IPA's data retention provisions did not comply with EU law and that the government should amend the legislation by November 2018. The law was amended in October 2018 to allow authorities to access the most intrusive non-content communications data (events data) only when investigating "serious crimes" (i.e., those with a 12-month minimum jail sentence) and to ensure that, in most cases, access to that data was independently authorized.

(II) fair trial rights.

Article 6 of the ECHR, as incorporated into UK domestic law through the HRA, provides for the right to a fair trial: "In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law."

According to the UK Country Report:

> [T]he law provides for the right to a fair and public trial, and an independent judiciary routinely enforced this right. Defendants enjoy a presumption of innocence, and the right to be informed promptly and in detail of the charges, with free interpretation as necessary from the moment charged through all appeals. Criminal proceedings must be held without undue delay and be open to the public except for cases in juvenile court or those involving public decency or security. Defendants have the right to be present at their trial. Under the Official Secrets Act, the judge may order the court closed, but sentencing must be public. Defendants have the right to communicate with an attorney of their choice or to have one provided at public expense if unable to pay. Defendants and their lawyers have adequate time and facilities to prepare a defense and free assistance of an interpreter if necessary. Defendants have the right to confront witnesses against them, present witnesses and evidence, and not to be compelled to testify or confess guilt. Defendants have the right to appeal adverse verdicts.

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

According to the UK Country Report, UK law:

> [P]rovides for freedom of expression, including for the press, and the government routinely respected these rights. An independent press, an effective judiciary, and

> a functioning democratic political system combined to promote freedom of expression, including for the press. [...] The law provides for the freedoms of peaceful assembly and association, and the government routinely respected these rights.

Article 10 of the ECHR, as incorporated into UK domestic law through the HRA, provides that "[e]veryone has the right to freedom of expression," which includes "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." However, Article 10 further indicates that the exercise of the right of freedom of expression is subject to certain formalities, conditions, restrictions or penalties "as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary." Based on Article 11 of the ECHR, as incorporated into UK domestic law through the HRA, no restrictions shall be placed on the exercise of the rights of freedom of assembly and association "other than such as prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others."

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. Certain UK laws on hate speech, such as the Public Order Act 1986 and speech-related provisions in the Terrorism Act 2006, are broadly worded and criminalize expression that in the United States would be considered protected speech under the First Amendment. Similarly, the Online Harms White Paper, released by the UK government in April 2019, sets forth broad plans for online safety measures, including regulations that would require technology companies to take precautions against illegal or "harmful" content and activity on their platforms. The broad scope of the proposed regulations may result in restrictions on freedom of expression in the United Kingdom that would not meet U.S. standards. There is no clear timeline for the UK government to introduce such regulations. The White Paper was followed by a public consultation, which finished on July 1, 2019. The United Kingdom will set out more detail on its proposals through a Government response to the consultation in the coming months. Despite these differences between the legal protections provided for in the United Kingdom and the United States, the United Kingdom maintains particularly strong and effective legal protections for freedom of expression, association, and peaceful assembly, as discussed in the UK Country Report.

In 2017, the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association issued a report on his mission to the United Kingdom where he commended the United Kingdom on its "sustained efforts at promoting and protecting the rights to freedom of peaceful assembly and of association ...," though noted more could be done, particularly with

respect to reversing measures that have negatively affected civil society's rights to freedom of association and assembly.[2]

(IV) prohibitions on arbitrary arrest and detention.

According to the UK Country Report, UK law "prohibits arbitrary arrest and detention and provides for the right of any person to challenge the lawfulness of his or her arrest or detention in court, and the government routinely observed these requirements." Article 5 of the ECHR, as incorporated into UK domestic law through the HRA, provides for the right to liberty and security of person. It further states that no one "shall be deprived of his liberty" except for in specifically enumerated situations, such as detention after conviction by a competent court, and "in accordance with a procedure described by law."

The United Nations High Commissioner for Refugees welcomed the United Kingdom's 2014 Parliamentary inquiry into Use of Immigration Detention in the UNHCR Global Strategy Beyond Detention 2014-2019. The inquiry has increased the scrutiny of detention centers in the United Kingdom.[3] Additionally, the United Kingdom has made positive developments to reduce arbitrary detention of stateless people, including the adoption of a statelessness determination procedure in 2013 and providing for a grant of leave for stateless persons to remain in the United Kingdom.

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

According to the UK Country Report, UK law prohibits torture and other cruel, inhuman, or degrading treatment or punishment, and there were no reports that government officials employed them.

The United Kingdom is a party to the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT). The United Kingdom 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 is a criminal offense in the United Kingdom under section 134 of the Criminal Justice Act 1988, with a maximum penalty of life imprisonment. Aiding and abetting torture is a criminal offence under section 8 of the Accessories and Abettors Act 1861 and subject to the same maximum penalty. Article 3 of ECHR, as incorporated into UK domestic law through the HRA, provides that no one shall be subjected to torture, inhuman or degrading treatment or punishment.

The United Kingdom submitted its 6th periodic report under the CAT in November 2017.[4] The UN Committee against Torture ("the Committee") concluded its consideration of the report in

---

[2] Maina Kiai, Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association on his Follow-up Mission to the United Kingdom of Great Britain and Northern Ireland, 8 June 2017, available at https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/28/Add.1

[3] UNHCR Global Strategy Beyond Detention 2014-2019, Oct 2015, available at https://www.unhcr.org/en-us/5631ee629.html

[4] Available at https://assets.publishing.service.gov.uk/.../uk-6th-periodic-report-under-cat.pdf

May 2019.[5] The report's primary concerns included the United Kingdom's failure to transpose all provisions of the CAT into domestic legislation; deficiencies in the approach to preventing torture and ill-treatment at home had led the United Kingdom to adopt policies that had caused it to fail to prevent torture beyond its territories in situations where its personnel exercised some degree of control; and the possible impact of Brexit on the United Kingdom's human rights framework. However, the Committee also noted a number of positive steps the UK government has taken to revise its legislation in areas of relevance to the CAT, including: the criminalization of forced marriage in England and Wales under the Anti-Social Behavior, Crime and Policing Act 2014; the enactment of the Serious Crime Act 2015 in England and Wales; the enactment of the Human Trafficking and Exploitation (Scotland) Act 2015; the introduction of the Limitation Act 2017; the adoption in 2014 of the Modern Slavery Strategy; the launch in 2014 of the Rape Action Plan; the implementation of Scotland's National Action Plan for Human Rights 2013-2017; the launch in 2016 and updating in 2018 of the Hate Crimes Action Plan (England and Wales); and the establishment in 2015 of the Independent Inquiry into Child Sexual Abuse. The Committee also noted its appreciation that the United Kingdom maintains a standing invitation to United Nation special mandate holders.

**18 U.S.C. § 2523(b)(1)(B)(iv): The United Kingdom has clear legal mandates and procedures governing those UK 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 UK entities authorized to seek data under the Agreement may do so under two distinct domestic legal authorities: the IPA, which, as discussed above, governs interception of live and stored communications for non-evidentiary purposes and interception or acquisition of metadata, and the Crime (Overseas Production Orders) Act 2019 c. 5 ("COPOA"), which authorizes production of data for evidentiary use in a court proceeding. Together with the UK Data Protection Act 2018 c. 12 (DPA), the IPA and the COPOA establish the procedures through which UK agencies collect, retain, use, and share data, as well as provide for effective oversight of these activities.

Investigatory Powers Act 2016:

The IPA authorizes specific UK government agencies to access communications' content (Part 2, Chapter 1) and non-content data (Part 3). For each authority, an IPA Code of Practice[6] describes in additional detail the legal parameters for IPA processes and safeguards for any data obtained under the IPA.

1. *Clear Legal Mandates and Procedures*

[5] Available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24578&LangID=E

[6] The Codes of Practice are issued pursuant to Schedule 7 of the IPA and, though not law, are admissible in evidence as evidence and take precedence over an agency's internal policies.

The IPA sets forth procedures for obtaining interception warrants and authorizations to obtain non-content communications data.[7] It identifies the public authorities, including law enforcement and intelligence agencies, that may apply for an interception warrant or obtain communications data authorizations under the IPA.[8] It sets the legal standard of necessity and proportionality that must be met for the Secretary of State to issue an interception warrant,[9] and it requires that, under the United Kingdom's new "dual lock" mechanism, a warrant must then be reviewed and approved by a Judicial Commissioner before it may take effect or, in emergency situations, within three working days of the warrant's issuance.[10] The IPA identifies entities authorized to access data collected through IPA warrants and imposes an obligation to protect the data from unauthorized disclosure.[11] The IPA also requires periodic reviews of the relevancy of stored data collected through IPA warrants and requires authorities to destroy data when there is no longer any relevant grounds for retaining it.[12] The DPA, as explained further below, governs access, use, and retention of personal data, including such data collected under the IPA.

2. *Effective Oversight*

The IPA is subject to review and oversight by the Investigatory Powers Commissioner (IPC) and his or her staff of Judicial Commissioners, inspectors, lawyers, and communications experts at the IPC Office ("IPCO"). The IPC is tasked with auditing, inspecting, and investigating the exercise of warrants under the IPA.[13] The IPC and Judicial Commissioners are appointed by the Prime Minister for three-year, renewable terms, upon joint recommendation by a group of four senior officials, three of whom are themselves judicial officials independent of the government.[14] They are removable only by a resolution passed by each House of Parliament or by the Prime Minister if the Commissioner has been the subject of specified legal actions, such as a criminal conviction or a bankruptcy order.

Crime (Overseas Production Orders) Act 2019:

The COPOA authorizes specified UK investigatory agencies to obtain electronic data exclusively for the purpose of investigating indictable offences or for the purpose of a terrorist investigation.[15] An overseas production order ("OPO") may only be granted when there is an international agreement in place between the United Kingdom and the country where the provider is located.[16]

1. *Clear Legal Mandates and Procedures*

---

[7] *See* IPA §§ 19–25, 30–38 (interception); *id.* §§ 60, 61, 63, 65 (communications data).
[8] *See id.* § 18 (interception warrants); *id.* §§ 70, 73 (communications data).
[9] *Id.* § 19 (interception warrants)
[10] *See id.* §§ 6, 23
[11] *Id.* §§ 53-59.
[12] *Id.* § 53.
[13] IPA § 229.
[14] IPA §§ 227 (1)-(4); 228(2), (3).
[15] COPOA § 2.
[16] COPOA § 1.

The COPOA authorizes identified UK agencies to seek OPOs from a judge only when the conditions and safeguards for domestic UK orders have been met.[17] All OPOs require that there are reasonable grounds for believing an indictable offence has been committed and that proceedings have been instigated in respect of that offence, or it is being investigated (or that the order is sought for the purposes of a terrorism investigation); that the data sought is likely to be of substantial value to the proceedings or investigation and that it is in the public interest for all or part of the data requested to be produced or accessed; that the application does not request excepted data—for example, legally privileged material or personal records that are confidential personal records, such as medical records.[18] As with data collected via domestic orders, data obtained through an OPO must be stored and shared in compliance with the DPA and may be retained for so long as necessary in all the circumstances.[19]

2. *Effective Oversight*

Judges grant production orders under the COPOA upon application by an authorized government entity, and those judges retain the authority to modify or revoke the order upon application by any person affected by the order or specified government authorities.[20] In addition, the IPCO—the same audit body for IPA warrants—will oversee use of OPOs pursuant to the Agreement.

UK Data Protection Act 2018:

The DPA and the European Union General Data Protection Regulation (GDPR),[21] which the DPA supplements and applies, together set forth a comprehensive legal framework for the private and public sector, including law enforcement and intelligence services, for the collection, retention, use, dissemination, and other processing of personal data, and for effective oversight of these processing activities, except where other laws take precedence.[22] The DPA also implements the EU Law Enforcement Directive.[23] The GDPR and Law Enforcement Directive are widely recognized as establishing strict data protection and privacy rules designed to implement protections in the Charter of Fundamental Rights of the EU[24] and Universal Declaration of Human Rights.[25] The DPA protects individuals with regard to the processing of

---

[17] COPOA § 4.
[18] COPOA § 1, 4.
[19] COPOA § 10(1).
[20] COPOA § 7.
[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).
[22] In the event that the UK exits the EU, the EU GDPR may no longer be law in the UK, depending on the terms of the departure from the EU.
[23] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Criminal Justice Directive).
[24] *See, e.g.*, Charter of Fundamental Rights of the European Union (2000/C 364/01) art. 7 (entitled "Respect for private and family life"), art. 8 (entitled "Protection of personal data").
[25] Universal Declaration of Human Rights, UN General Assembly Resolution (1948) art. 12 ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks").

their personal data by requiring personal data to be processed lawfully and fairly based on certain specified bases, conferring certain rights on the data subject, setting up governance and accountability mechanisms, and establishing a supervisory authority, the Information Commissioner, with responsibility for monitoring and enforcing the DPA.[26]

*1. Clear Legal Mandates and Procedures*

The DPA sets forth key data protection principles related to the collection, use, processing, retention, and dissemination of personal data. When personal data is processed for a law enforcement purpose, that purpose must be specified, explicit, and legitimate; the data processed must be adequate, relevant and not excessive in relation to the purpose; the data must be kept for no longer than necessary for the purpose for which it is processed; and appropriate time limits must be established for periodic review of the need for continued storage.[27] Using appropriate technical and organization measures, personal data must be processed in ways that ensure a level of security appropriate to the risks and include measures designed to prevent unauthorized processing, and data controllers and processors must retain logs of processing operations, including alteration or disclosure of data.[28] They also must implement data protection "by design" and "by default," including data minimization measures.[29] The DPA also imposes restrictions on transfers outside of the European Union—permitting transfer for example in cases where the transfer to a third country is necessary for law enforcement purposes and the recipient is a relevant law enforcement authority.[30]

Certain provisions of the DPA require the data controller to implement policies for complying with the DPA's terms.[31] For example, the DPA requires a specific policy for "sensitive processing" as a safeguard for the processing of data that reveals race, political opinions, religious beliefs, or involves health, genetic or biometric data.[32] The policies must explain procedures for compliance with the data protection principles and for retention and erasure of such data, and tying into governance and accountability measures, the policy must be reviewed and updated as needed, and made available to the Information Commissioner upon request.[33]

Data subjects also have certain rights that controllers and processors must fulfill, for example, to information, access, rectification of inaccurate data, and erasure or restriction of processing.[34] Controllers must make certain information available to data subjects, either by making it generally available to the public or through other means, including the identity and contact details of the data controller, purposes for which the controller processes data, contact details of the data protection officer, and existence of data subject rights.[35] Additional notices are required

---

[26] UK Data Protection Act 2018 (DPA), Art. 2, Protection of personal data. Because the DPA references specific provisions of the GDPR and Law Enforcement Directive, citations will generally only refer to the DPA.
[27] DPA §§ 36, 37, 39.
[28] DPA §§ 40, 62, 66.
[29] DPA § 57.
[30] DPA §§ 73, 76.
[31] *See, e.g.*, DPA § 42.
[32] DPA § 42.
[33] *Id.*
[34] DPA §§ 45-47.
[35] DPA § 44(1).

in specific cases, including information on the legal basis for processing, period of time the data will be retained, and categories of recipients of the data.[36]

A controller may restrict data subject rights in certain situations involving protection of public safety, for example to avoid prejudicing official lawful investigations and to protect public security. The DPA appropriately confines such restrictions, and provides that restrictions may only be used to the extent that, and for so long as, the restriction is a "necessary and proportionate" measure to avoid obstructing an official inquiry, avoid prejudicing the prevention, detection, investigation or prosecution of criminal offenses, to protect public security or national security, and protect the rights and freedoms of others.[37] In these situations, the data controller needs to inform the data subject about the restrictions, including the data subject's right to make a complaint about the restrictions, except when informing the data subject would undermine the purpose of the restriction, e.g., to protect public security.[38] The controller must record the reasons for the restriction and, if requested, make the record available to the Information Commissioner.[39]

2. *Effective Oversight*

The DPA requires controllers and processors to implement appropriate measures that ensure and demonstrate compliance. They must put into place "comprehensive but proportionate" accountability and governance measures.[40] One such measure is the requirement that data controllers, excluding judicial authorities, designate data protection officers who bear certain specified responsibilities and should not be dismissed or penalized for exercising their duties.[41] Other measures include the policies referenced above, requirements that entities maintain documentation on processing activities, and that entities conduct data protection impact assessments when the type of processing "is likely to result in a high risk to the rights and freedoms of individuals."[42]

Regarding oversight, the UK Information Commissioner has supervisory authority to monitor and enforce the DPA, advise the Parliament and other parts of the UK government, handle complaints, conduct investigations, receive notices of and investigate data breaches, inspect personal data and processing operations, and review and approve certain mechanisms for data transfers.[43] The Information Commissioner is also the UK authority responsible for monitoring the law enforcement provisions in DPA Part 3, and the application of the EU Law Enforcement Directive.[44] Overall, the DPA, along with the IPA and COPOA, provide clear legal mandates and procedures governing the UK entities that are authorized to seek data under the Agreement, including procedures through which such entities collect, retain, use, and share data, with effective oversight of these activities.

---

[36] DPA § 44(2).
[37] DPA § 45.
[38] DPA §§ 45(4)-(6).
[39] DPA § 45(7).
[40] Guide to Law Enforcement Processing, UK Information Commissioner's Office, at 37, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.
[41] DPA §§ 69-71.
[42] DPA §§ 64, 67.
[43] DPA Part 5.
[44] DPA, §§ 115-116.

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

UK 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 the United Kingdom's collection and use of electronic data collected pursuant to the Agreement.

UK Data Protection Act 2018 and the Crime (Overseas Production Orders) Act 2019:

As with data collected via domestic orders, data obtained through an OPO issued under COPOA must be stored and shared in compliance with the DPA and may be retained for so long as necessary in all the circumstances.[45] As explained above, the DPA contains mechanisms to provide accountability and transparency regarding collection and use of electronic data. Data controllers must make certain information available to data subjects, including the identity and contact details of the data controller, purposes for which the controller processes the data, and how to lodge complaints.[46] As to accountability, the controllers must maintain data protection officers and ensure that those officers are "involved, properly and in a timely manner, in all issues which relate to the protection of personal data," and have necessary resources and access to personal data and processing operations to fulfill their functions.[47]

In addition, the DPA, following the GDPR, establishes the UK Information Commissioner to perform oversight functions, to include audit, inspection, and investigation, and enforcement in relation to data controllers and processors, as explained above.[48] This includes oversight of the government's collection and use of data pursuant to OPOs.[49] To carry out this mandate, the DPA grants the Information Commissioner a variety of powers to investigate and enforce, including the ability to demand documents and other information from data controllers, including law enforcement agencies authorized to collect that information.[50] Indeed, the Information Commissioner's Office (ICO) regularly exercises its powers over law enforcement agencies.[51] Each year the ICO makes a yearly report to the Parliament and the public.[52]

Although COPOA does not impose a mandatory expiration date for non-disclosure orders that preclude notice to the target of an order, as part of the agreed targeting and minimization procedures for OPO subject to the Agreement, discussed below, the United Kingdom requires Orders to specify or describe when its non-disclosure requirement expires.

---

[45] COPOA § 10(1), DPA §§ 39, 57(4).
[46] DPA §44(1).
[47] DPA § 71.
[48] DPA pt 5.
[49] *See* DPA §§ 115, 116 and Schedule 13.
[50] *See* DPA §§ 142-144, 154 and Schedule 15.
[51] For example, the ICO's oversight authority includes the ability to issue monetary penalties for failure to comply with Part 3 of the DPA that deals with law enforcement processing of personal information. ICO enforcement actions over law enforcement agencies, as well as other data controllers, can be found here: https://ico.org.uk/action-weve-taken/enforcement/.
[52] *See* DPA § 139.

Investigatory Powers Act:

The DPA governs access, use, and retention of personal data, including data collected under the IPA. In addition, the IPA and IPA Codes of Practice further specify government access, use, and retention of data collected under the IPA. The IPA also sets forth an inspection and audit regime to safeguard against abuses of power by the government when collecting and intercepting stored and real-time communications. The IPC has a mandate to perform oversight—including "audit, inspection and investigation"—of the government's "interception of communications" and "acquisition or retention of communications data."[53] To carry out this mandate and effectively monitor public officials' accessing of real-time and stored communications, the IPA also gives the IPC expansive powers to investigate and demand documents and other information from government personnel authorized to collect that information.[54] The IPA requires that the IPC make a yearly report to the Prime Minister.[55] The Prime Minister must make the report public, unless there is a statutory basis (e.g., national security, economic well-being of the United Kingdom, etc.) to exclude certain provisions from publication.

In addition to the work of the IPC, the Investigatory Powers Tribunal is an independent UK court established in 2000 that decides complaints about the conduct of the UK intelligence agencies, including claims asserting violations of the HRA.

The IPA has been subject to a series of legal challenges in the United Kingdom since it passed in 2016. In 2018, the UK High Court ruled that the IPA provisions regarding "retention notices" to telecommunications operators requiring the retention of data were lawful but that elements of the provision regarding communications data acquisition did not comply with EU law as drafted.[56] The UK government had already conceded those elements of the claim and the failings identified in the ruling were subsequently addressed by the Data Retention and Acquisition Regulations 2018. In 2019, the UK High Court rejected a claim that the IPA provisions regarding "bulk" powers were incompatible with the HRA.[57]

**18 U.S.C. § 2523(b)(1)(B)(vi) The United Kingdom 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 UK Country Report:

> The 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 country has no blanket laws covering internet blocking, but the courts have issued blocking injunctions against various categories of content such as depictions of child sexual

[53] IPA ¶ 229(1)(a)-(b).
[54] *See* IPA ¶ 235.
[55] *Id.* ¶¶ 234, 231.
[56] R (National Council for Civil Liberties) v Secretary of State for the Home Department [2018] EWHC 975 (Admin); [2019] QB 481
[57] R (National Council for Civil Liberties) v Secretary of State for the Home Department [2019] EWHC 2057 (Admin).

abuse, promotion of extremism and terrorism, and materials infringing on copyrights. By law, the electronic surveillance powers of the nation's intelligence community and police allow them, among other things, to check internet communications records as part of an investigation without a warrant.

In addition, the United Kingdom has no law requiring that certain categories of data, such as data pertaining to UK citizens, be stored or processed in the United Kingdom, and the United Kingdom has opposed the adoption by other countries of such data localization laws.

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

The United Kingdom has adopted procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons that the United Kingdom acquires under the Agreement. Article 7 of the Agreement requires the United Kingdom to adopt these procedures and sets forth restrictions the procedures must contain, also reflecting targeting and minimization requirements set forth in 18 U.S.C. § 2523(b)(4) discussed below. The United Kingdom has adopted two sets of procedures for use with "Orders," as defined in the Agreement, one set of procedures for use with Orders issued pursuant to the COPOA, the other for use with Orders issued pursuant to the IPA. The types of Orders the United Kingdom may issue subject to the Agreement under the COPOA and IPA are discussed below. Both the COPOA procedures and the IPA 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 both 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) the United Kingdom 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) the United Kingdom 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;**

The United Kingdom's procedures contain targeting restrictions to minimize the acquisition of information concerning United States persons that the United Kingdom 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 the United Kingdom 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) the United Kingdom 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 the United Kingdom 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 the United Kingdom 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 8(3) of the Agreement prohibits the United Kingdom 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 the United Kingdom's sharing of data with the United States government. Specifically, the procedures state that the content of a communication of a United States person shall not be disseminated to the United States, unless the communication can be disseminated pursuant to the dissemination standards 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.

**(D) an Order issued by the United Kingdom under the Agreement –**

The Orders the United Kingdom may issue under the Agreement satisfy 18 U.S.C. § 2523(b)(4)(D), which sets forth six procedural safeguards and other limitations, some of which must be given effect under United Kingdom domestic law. The United Kingdom will invoke the Agreement only with respect to Orders authorized by the COPOA and the IPA. Under the COPOA, the United Kingdom will invoke the Agreement with respect to OPOs. Under the IPA, the United Kingdom will invoke the Agreement only with respect to "targeted interception warrants" authorized by IPA Part 2 to obtain the content of electronic communications data, and "communications data authorizations" authorized by IPA Part 3 to require providers to disclose different types of non-content communications data, including the type that may be obtained via pen register or trap and trace devices ("PRTT data") under 18 U.S.C. Chapter 206. The United

Kingdom will not, in contrast, invoke the Agreement with respect to other parts of the IPA, such as "bulk interception warrants" authorized by IPA Part 6. The following explains how each type of Order the United Kingdom may issue under the Agreement 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 United Kingdom legislation and procedures. Both the COPOA and the applicable IPA sections authorize the issuance of Orders for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of crime including Serious Crime, which is defined in the Agreement as an offense punishable by a maximum term of imprisonment of three years or more, including terrorist activity.[58] The procedures further require that Orders may only be issued for the purpose of obtaining information relating to the prevention, detection, investigation or prosecution of a Serious Crime. The procedures also require the United Kingdom 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 United Kingdom legislation and procedures. The COPOA requires that OPOs specify or describe the electronic data sought.[59] The COPOA procedures further require that the United Kingdom will only issue overseas production orders against specific identifiers. IPA Part 2 requires that targeted interception warrants specify the "factors," such as the addresses, numbers, or apparatus, that will be used to identify communications likely to be from or intended for the persons, organizations, or premises named or described in the warrant.[60] IPA Part 3 requires that communications data authorizations specify or describe the non-content data to be obtained.[61] The IPA procedures further require that the United Kingdom will only issue Orders under the IPA against specific identifiers.

> (iii) shall be in compliance with the domestic law of the United Kingdom, 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;

---

[58] COPOA § 4(3); IPA §§ 20(2), 61(7)(b).
[59] COPOA § 1(2)(b).
[60] IPA § 31(8).
[61] IPA § 64(1)(d).

The first requirement is addressed by Article 5(1) of the Agreement, which requires that United Kingdom Orders subject to the Agreement shall be issued in compliance with United Kingdom law, and by Article 5(7), which further requires that each United Kingdom Order subject to the Agreement must include a written certification by the United Kingdom'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 United Kingdom Orders derives solely from United Kingdom 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 United Kingdom legislation and procedures. The COPOA requires that the judge issuing an OPO must be satisfied that there are reasonable grounds to believe that the data specified or described is likely to be of substantial value to a specified criminal proceeding or investigation or a terrorism investigation, that the data is likely to be relevant evidence to any criminal proceeding or investigation specified in the application, and that production of the data is in the public interest, having regard to the benefit likely to accrue to a specified criminal proceeding or investigation or a terrorism investigation.[62] Targeted interception warrants under IPA Part 2 and communications data authorizations under IPA Part 3 must be issued based on findings that the warrant or authorization is "necessary" based on the specified purpose and that the conduct the warrant authorizes is "proportionate" to what is sought to be achieved.[63]

> (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 United Kingdom legislation and procedures. OPOs may only be issued by independent judges of the United Kingdom.[64] Targeted interception warrants issued under IPA Part 2 and subject to the Agreement are subject to review and oversight by Judicial Commissioners, who are independent of the government and operate in the Investigatory Powers Commissioner Office ("IPCO"), which as discussed above is an entity established by the IPA to exercise independent review and oversight functions.[65] Communications data authorizations issued under IPA Part 3 and subject to the Agreement will either be authorized by the Office for Communications Data Authorizations on behalf of IPCO or subject to review and oversight by Judicial Commissioners.

---

[62] COPOA § 4(5)-(7).
[63] IPA §§ 23, 60A(1), 61(1).
[64] COPOA § 1(1).
[65] IPA § 23.

(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 live interception of communications that are issued under the IPA must comply with these requirements based on provisions set forth in the IPA procedures. These restrictions are not set forth in the COPOA procedures, as OPOs may not be issued for the live interception of communications.

**(E) an Order issued by the United Kingdom 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 8(4) provides that where the United Kingdom 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 the United Kingdom in a manner which raises freedom of speech concerns for the United States, then the United Kingdom 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 United Kingdom statutes that may raise freedom of speech concerns and other circumstances under which such concerns may arise, and provides that the United States may unilaterally supplement that list of statutes.

**(F) the United Kingdom 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 the United Kingdom 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) the United Kingdom 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 the United Kingdom 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) the United Kingdom 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 the United Kingdom from disseminating to United States authorities the content of a communication of a United States person that the United Kingdom 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) the United Kingdom 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 United Kingdom laws would otherwise prohibit communications service providers from disclosing the data;**

Article 3(1) of the Agreement provides that the United Kingdom 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 United Kingdom law, for example through IPA provisions permitting providers to disclose data in response to a data request made under a designated international agreement. Additionally, with respect to restrictions on the preservation, authentication, disclosure, and production of data that may arise from data protection legislation, the Agreement addresses in Articles 2 and 9(1) the main relevant legal bases under applicable data protection legislation for data processing and transfer required for the execution of Orders. Article 9(2) confirms that processing and transfer of data in the execution of Orders subject to the Agreement are compatible with United Kingdom law, including data protection law made part of United Kingdom law as a Member State of the European Union.

**(J) the United Kingdom 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 12(1) of the Agreement. The Department of Justice will conduct periodic reviews of the United Kingdom's compliance with the terms of the Agreement and both sets of targeting and minimization procedures. To support these compliance reviews, in the first instance, both sets of procedures require United Kingdom agencies issuing Orders subject to the Agreement to record and report certain breaches or instances of noncompliance with the procedures and the Agreement. The United Kingdom will then report instances of noncompliance to the Department of Justice. The procedures also require the United Kingdom's Investigatory Powers Commissioner to conduct periodic audits of the United Kingdom'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 the United Kingdom to remedy them. In addition, through reviewing the information provided by the United Kingdom regarding instances of noncompliance, the Department of Justice will look to identify trends in compliance

issues and determine through discussions with the United Kingdom 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 the United Kingdom has not properly invoked the Agreement with respect to any Order, it shall notify the United Kingdom 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. Additionally, under Article 11(3) of the Agreement, if the United States and the United Kingdom are unable to resolve a relevant concern or dispute, the United States may notify the United Kingdom that the Agreement may not be invoked with respect to an identified category of Orders, including Orders issued on or after a particular date, pending notification by the United States that it has revoked its conclusion.