

INTRODUCTORY NOTE TO 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
BY KENNETH PROPP*
[October 3, 2019]

Introduction

On October 3, 2019, the United States and the United Kingdom signed an innovative international agreement on international assistance in criminal matters.¹ The agreement, which has not yet entered into force, will enable law enforcement authorities in either country to request and obtain electronic communications content data directly from service providers located in the other country. It is intended to obviate the need, with respect to e-evidence, for resort to the slower and more cumbersome mutual legal assistance treaty (MLAT) in force between the two countries.²

Background

Under an MLAT, a law enforcement investigator or prosecutor seeking foreign-located evidence needed for a domestic criminal proceeding sends a request through a designated central authority in their home state to a foreign counterpart authority, which ensures its execution under foreign criminal procedure law. Such centralized mediation in the receiving state unavoidably adds considerable time to execution of an MLAT request. Technological developments in recent years have added to the strain on the MLAT system. The rapid proliferation of electronic communications and documents, combined with the advent of cloud computing, enables information relevant to a criminal investigation to be stored easily outside national borders—indeed, anywhere in the world.³

Since U.S. companies provide most of the electronic communications and cloud storage services utilized abroad, and they typically store foreign-origin data in servers in the United States, the burden on the U.S. government of responding to MLAT requests has risen rapidly. The U.S. Department of Justice acknowledged publicly that the average response time to an MLAT request was nine months.⁴ In 2018, Congress responded to the problem by enacting the Clarifying Lawful Overseas Use of Data Act (CLOUD Act),⁵ which authorized the executive branch to conclude binding international agreements specifically designed to enable more rapid access to e-evidence located in the United States or abroad.⁶

The CLOUD Act fundamentally changed the MLAT paradigm by eliminating a governmental executing role for a request for e-evidence received from foreign law enforcement; instead, a law enforcement agency sends a request *directly* to a service provider in the other country. The law balanced this procedural short-cut by setting strict requirements for the content of the request, including that it be targeted to specific accounts, addresses, or persons; subject to review or oversight by a judge, magistrate, or other independent authority in the sending state; and based on articulable and credible facts.⁷

UK–U.S. CLOUD Act Agreement

The UK–U.S. CLOUD Act Agreement is the first fruit of the new U.S. statutory empowerment. It incorporates not only the CLOUD Act stipulations, but also a series of additional safeguards. Among them are: an opportunity for the service provider to object to the requesting foreign state when the service provider believes that the Agreement is being improperly invoked; a limitation in scope to cases of serious crimes penalized by three years' or more imprisonment; and notifications of requests to affected third-country governments.⁸ Each government also won the right to veto the use of e-evidence obtained from its territory in the other's criminal proceedings in specific circumstances: the United Kingdom in a U.S. case in which the death penalty is sought, and the United States in a UK case raising freedom of speech concerns.⁹

*Kenneth Propp teaches European Union law at Georgetown University Law Center and is a fellow at the Atlantic Council's Future Europe Initiative.

The UK–U.S. Agreement does not serve as the sole means for obtaining e-evidence located in the territory of the other state, however. Article 11(1) of the UK–U.S. Agreement provides that it “is without prejudice to and shall not affect other legal authorities and mechanisms” for obtaining evidence, including requests for mutual legal assistance.¹⁰ Also undisturbed are existing U.S. unilateral extraterritorial powers for obtaining e-evidence.¹¹

The United States did not need to make changes to domestic law in order to implement the UK–U.S. Agreement, since the CLOUD Act itself had already effected the necessary reforms.¹² Notably, the CLOUD Act lifted the bar in the Stored Communications Act that previously had precluded a communications service provider from disclosing content data in response to a foreign government request, replacing it with a provision permitting disclosure pursuant to a CLOUD Act executive agreement.¹³

The United Kingdom, on the other hand, required more extensive domestic legal change to give effect to this new kind of agreement for providing international judicial assistance. In the Crime (Overseas Production Orders) Act 2019, Parliament granted law enforcement agencies and prosecutors the power to seek and obtain electronic communications content data directly from service providers, so long as it is done on the basis of a relevant UK international agreement, and also created a new type of overseas production order for this purpose.¹⁴

Conclusions

The UK–U.S. Agreement has had a mixed reception internationally. Law enforcement agencies around the world regard it as an extremely promising avenue for enabling rapid and efficient access to U.S.-located electronic evidence needed for prosecuting even the most domestic of crimes. Many countries reportedly have clamored to pursue CLOUD Act agreements with the United States, and several negotiations are underway. Those with Australia are said to be close to completion,¹⁵ and talks with other members of the “Five Eyes” intelligence collective—Canada and New Zealand—may well follow in due course. The United States also has commenced discussions with the European Union, which are at an early stage.¹⁶

Civil libertarians and privacy advocates, however, have criticized the approach of CLOUD Act international agreements for not incorporating the same panoply of judicial and central government controls as MLATs. They are uneasy at the new power afforded to foreign criminal investigators and prosecutors to directly obtain foreign-located e-evidence and regard the due process and other procedural safeguards incorporated into the CLOUD Act and the UK–U.S. Agreement as insufficient. This debate remains unresolved, particularly in Europe.¹⁷

The UK–U.S. Agreement represents an important conceptual evolution in international criminal assistance law to meet the extraterritorial challenges of e-evidence; however, it is too soon to say whether its approach will be embraced widely in future international agreements.

ENDNOTES

- 1 Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime [hereinafter UK–U.S. CLOUD Act Agreement], UK–U.S., Oct. 3, 2019.
- 2 Treaty on Mutual Legal Assistance in Criminal Matters, UK–U.S., Jan. 6, 1994, T.I.A.S. No. 96-1202 (entered into force Dec. 2, 1996). *See also* Instrument as contemplated by Article 3(2) of the Agreement on Mutual Legal Assistance, U.S.–EU, June 25, 2003, as to the application of the Treaty on Mutual Legal Assistance in Criminal Matters of January 6, 1994, Dec. 16, 2004, T.I.A.S. No. 10-201.48 (entered into force, Feb. 1, 2010).
- 3 A recent European Commission study estimated that a very large majority (85%) of member state criminal investigations today require electronic evidence in some form, and in two-thirds of the cases such evidence is in the hands of online service providers based in another jurisdiction. *See* European Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceeding (2018), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN>.
- 4 *Liberty and Security in a Changing World*, President’s Review Group on Intelligence and Communications Technology, p. 227 (Dec. 12, 2013).
- 5 Clarifying Lawful Overseas Use of Data Act, contained in Consolidated Appropriations Act, 2018, P.L. 115–141, div. V [hereinafter CLOUD Act].

- 6 As a matter of U.S. treaty law, CLOUD Act agreements are considered to be executive agreements. The U.S. executive must submit to Congress a series of certifications that a CLOUD Act agreement fulfills certain privacy and due process requirements, and the Congress is afforded a mandatory period to review the agreement before it may enter into force. CLOUD Act, *id.*, § 105 (adding 18 U.S.C. 2523(d)). See Theodore Christakis & Kenneth Propp, *The Legal Nature of the UK–US CLOUD Agreement*, CROSS-BORDER DATA FORUM (Apr. 20, 2020), <https://www.crossborderdataforum.org/the-legal-nature-of-the-uk-us-cloud-agreement>.
- 7 CLOUD Act, *supra* note 5, § 105 (adding 18 U.S.C. 2523(b)).
- 8 For a fuller discussion of the significant features of the agreement, see Jennifer Daskal & Peter Swire, *The UK–US CLOUD Act Agreement is Finally Here, Containing New Safeguards*, LAWFARE AND JUST SECURITY (Oct. 8, 2019), <https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards>.
- 9 UK–U.S. CLOUD Act Agreement, *supra* note 1, art. 8(4).
- 10 The UK’s internal explanatory memorandum bluntly states that “(t)he UK–U.S. Mutual Legal Assistance Treaty is not changed by the Agreement and remains in place.” This reflects that there may well be circumstances in which limitations contained in the CLOUD Act agreement—targeting limitations, or restrictions on the scope of covered offenses, for example—compel law enforcement authorities in the United States or United Kingdom to resort to the MLAT instead. See Explanatory Memorandum to the UK–U.S. Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime, Cm. 178 (2019).
- 11 The United States possesses such powers under a separate part of the CLOUD Act itself, which clarified that a provider of electronic communications services is obliged to disclose to the U.S. Government, pursuant to warrant, content data within its possession, custody or control, even if located outside the United States. CLOUD Act, *supra* note 5, § 103 (amending 18 U.S.C. 2713).
- 12 The Department of Justice has taken a subsequent administrative step relating to designation of the United Kingdom under the Agreement, a prerequisite to bringing the agreement into force. See 85 Fed. Reg. 67568 (Oct. 23, 2020).
- 13 CLOUD Act, *supra* note 5, § 104 (amending 18 U.S.C. 2511(2)).
- 14 Crime (Overseas Production Orders) Act 2019, Chapter 5. The UK Secretary of State subsequently designated the UK–U.S. Agreement under the powers conferred by the 2019 law. See Overseas Production Orders and Requests for Interception (Designation of Agreement) Regulations 2020, c. 38 (UK) (Jan. 16, 2020).
- 15 U.S. Dep’t Just., Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton (Oct. 7, 2019), <https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us>.
- 16 See Peter Swire, *EU and U.S. Negotiations on Cross-Border Data, Within and Outside of the Cloud Act Framework*, LAWFARE (Apr. 13, 2019), <https://www.crossborderdataforum.org/eu-and-u-s-negotiations-on-cross-border-data-within-and-outside-of-the-cloud-act-framework>. The EU simultaneously is in the process of developing its own e-evidence legislation, and it may prefer that an agreement on this subject with the United States not be an executive agreement within the framework of the CLOUD Act.
- 17 For example, a recent study by a major EU policy think-tank calls for the European Union to rely solely on mutual legal assistance treaties to govern evidentiary matters with the United States, and to abandon pursuit of an e-evidence agreement. See SERGIO CARRERA, MARCO STEFAN, VATSAMIS MITSILEGAS (RAPORTEURS), CROSS-BORDER DATA ACCESS IN CRIMINAL PROCEEDINGS AND THE FUTURE OF DIGITAL JUSTICE, Center for European Policy Studies (Oct. 2020) 77.

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*
[October 3, 2019]

**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.

*This text was reproduced and reformatted from the text available at the U.S. Department of Justice website (visited December 8, 2020), <https://www.justice.gov/dag/cloud-act-agreement>.

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 11.⁷
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 this 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 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: