

Explanatory Memorandum 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

Title

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

Command Paper No: 178

Subject Matter

1. Increasingly, terrorists and criminals are using global communications services, including social media applications, to facilitate their criminal activities. This makes the data generated by those applications a vital source of evidence for the investigation and prosecution of serious crimes, including terrorism offences. However, the companies providing these services, or processing the data generated from using them, are often located outside the UK, primarily the US. It is an essential tool in the fight against child sexual exploitation and abuse.
2. Currently, due to barriers in US law, access by UK law enforcement and prosecution authorities to the communication content held by US Communications Service Providers (CSPs) for evidential use in investigations and prosecutions is only possible using the US/UK Mutual Legal Assistance (MLA) Treaty, a form of judicial co-operation. Obtaining this data via the MLA treaty requires considerable resources, in the UK and the US, to expedite the request as detailed consideration is needed to satisfy the US that the request meets the terms of the treaty. In practice this means that the data requested is provided many months after the request is made. The total time for the process is typically a year but can be years. Meanwhile the criminal activity continues with victims continuing to be harmed. Furthermore, innocent people can remain under suspicion as there is not the evidence to eliminate them from the investigation.
3. UK national security agencies are also constrained by the same barriers in US law with access to content data held by the US CSPs only possible where there is an exigent threat to life. Hence there is significant data which is not available to them to support their investigations.

4. Enabling cross-border access to this information has been a high priority for the UK Government and UK law enforcement and national security agencies for a number of years.
5. This Agreement, when brought into force, will enable national security, law enforcement and prosecution agencies to make requests, using the appropriate legal process under the law of the country making the request, to the CSP who holds the data, providing the requirements in the Agreement are met.
6. This Agreement will facilitate the reduction in the possibility of investigations or prosecutions being delayed or abandoned due to an inability to access to data.
7. The Agreement does not compel a CSP in the other party's jurisdiction to comply with a request. Any actions taken in the event of non-compliance are governed by the legislation of the country making the request.
8. The Agreement however places obligations on the two countries remove the barriers in domestic law within the jurisdiction the CSP is located which would otherwise prevent disclosure of this data recognised by this Agreement.
9. The Agreement works alongside existing legislation in both countries and requires the respective Governments to amend or create domestic legislation where this is necessary to do so to give effect to the terms of the Agreement.
10. The Agreement requires each party to comply with their own domestic legislation when making a request for Covered Data.
11. Orders for data can only be made under the Agreement for the purpose of the prevention, detection, investigation or prosecution of a serious crime (including terrorism). A serious crime is defined as one which could result in a custodial sentence with a maximum possible term of at least 3 years. For other types of request recognised by the Agreement, a lower threshold of being for the purpose of the prevention, detection, investigation or prosecution of crime must be met.
12. Orders under the Agreement must be for Covered Data which means the following types of data: the 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. This data must be held or processed by the CSP.
13. The Agreement recognises that requests can be made for subscriber information which is defined as information that identifies a subscriber or customer of a CSP, 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.
14. When the UK is using the Agreement, they cannot request Covered Data on a US Person or a person located in the US. For requests made by the US to a UK CSP, the person must not be located in the UK. This differentiation results from EU law

which prohibits discrimination in treatment between citizens of different member states.

15. The Agreement requires that each party have a Designated Authority, who is responsible for serving Order based requests directly to the CSP and forwards requested data to the requesting public authority.
16. The Agreement cannot be used for Orders on behalf of another government and the UK cannot make request on behalf of the US and vice versa. Permission must be obtained from the other party, if the requesting party wishes to share the data with another country or international organisation. Furthermore, there is no compulsion under the Agreement to share data obtained under the Agreement with the other party or any third party.
17. The Agreement does not compel the CSP to remove encryption and is encryption neutral.
18. The Agreement itself does not compel a CSP to comply with the request. Any actions taken in the event of non-compliance are governed by the legislation of the country making the request.
19. To remain aligned with the UK policy regarding the death penalty, the Agreement includes that, in the event that data obtained from a UK CSP is intended to be used as evidence in a case which could result in the death penalty, the US will obtain permission from the UK to use this data in evidence before doing so. In this event the UK will undertake an assessment under the OSJA process to inform the UK minister's decision.
20. Also, to remain aligned with the 1st Amendment to the US Constitution, the Agreement includes that, in the event that data obtained from a US CSP is intended to be used in evidence in a case where the US position on freedom of speech raises potential issues as regards the use of such data in a prosecution, then the UK will obtain permission from the US to use this data in evidence before doing so.
21. This Agreement is without prejudice to other means by which each party might obtain data. The UK/US Mutual Legal Assistance Treaty is not changed by the Agreement and remains in place.
22. The Agreement specifies that requests made under the Agreement are compatible with each country's respective applicable laws regarding privacy, freedom of information and data protection. The Agreement, because of the data protection safeguards it contains, including through incorporation of the DPPA, provides appropriate safeguards as a legally binding and enforceable instrument between public authorities or bodies under Article 46(2)(a) of the GDPR.
23. The Agreement makes provision for mutual review of operation of the Agreement. Each country's designated authority is required to issue an annual report on the operation of the Agreement.

24. The Agreement also provides for a process to handle issues arising from the operation of the Agreement and the resolution of these issues.
25. The Agreement will be brought into force through the exchange of diplomatic notes.
26. The Agreement will remain in force for five years, and can be extended by mutual agreement for five years (or any other period as may be agreed).

Ministerial Responsibilities:

The Secretary of State for the Home Department

- Has overall responsibility for the conclusion and implementation of this Agreement;
- Has overall responsibility for the detection, prevention, and investigation of serious crime and its relevant legislation.

The Minister of State for Security and Economic Crime

Has responsibility for:

- The ratification and designation of this Agreement;
- Investigatory powers and relevant legislation (including the Investigatory Powers Act 2016; the Crime (Overseas Production Orders) Act 2019;
- Serious organised crime, economic crime, and National Crime Agency oversight;
- Counter-terrorism

The Attorney General

- Has overall responsibility for the prosecution of serious crime.

The Secretary of State for Foreign & Commonwealth Affairs

- Has overall responsibility for United Kingdom policy relating to the United Kingdom's relations with the United States of America;
- The Overseas Security and Justice Assessment process.

Policy Considerations:

(i) General

Enabling cross-border access to this information has been a high priority for the UK Government and UK law enforcement and national security agencies for a number of years. In recognition of this challenge, the UK prime minister in 2014 appointed Sir Nigel Sheinwold as a special envoy tasked with working with the US government to establish data access arrangements. The need for improved access to data also formed one of the recommendations made by Lord Anderson QC in 2016 in his report entitled “A Question of Trust¹” where he advised the government to:

“take a lead in developing and negotiating an new international framework for data-sharing among like minded democratic nations”

The UK-US Agreement is the first of these cross border agreements. When brought into force, it will enable UK national security, law enforcement and prosecution agencies to make requests, using an appropriate authorised UK order, directly to the US CSP who holds the data, providing the requirements in the Agreement are met. This will remove the barriers in US law to US CSPs acting upon UK orders.

This Agreement will facilitate the reduction in the possibility of investigations or prosecutions being delayed or abandoned due to an inability to access to data. Furthermore, it will improve the speed in eliminating people from an investigation.

This Agreement will also enable US law enforcement agencies to make requests directly to UK CSPs for data. However, it is anticipated that the US will make considerably less use of the Agreement as few UK CSPs hold data of interest to the US. The reduction in the burden on the US from MLA treaty requests is the key benefit the Agreement will deliver to the US.

The Agreement has taken over 4 years to negotiate with commitment from the UK Prime Minister and the US President to enter into an Agreement. It has required both the US and the UK to introduce changes to legislation to remove legislative barriers as well as agree the terms of the Agreement itself. Hence significant effort has been expended by both sides to conclude this Agreement which is a testament to the value the UK attaches to this Agreement in obtaining access to data which may not otherwise be available.

The US enabling legislation, the Clarifying Lawful Overseas Use of Data (CLOUD) Act, allows US CSPs to comply with requests by another country for content data,

¹ A Question of Trust issued in December 2016 by David Anderson QC, recommendation made in chapter 15 Recommendations Para 7.66

provided an Agreement is in place. It was approved by the US President on 23 March 2018. The UK also passed legislation to address barriers in UK law:

1. The Data Retention and Investigatory Powers Act 2014 and the Investigatory Powers Act 2016 made orders authorised under these acts extraterritorial. It also removed the barrier to UK CSPs responding to requests from another country for data, providing an international agreement was in place between the UK and the other country.
2. The Crime (Overseas Production Orders) Act 2019 provided UK law enforcement and prosecution agencies with the power to apply to UK courts for overseas production orders with extra-territorial effect providing there was an international agreement in place between the UK and the other country.

(ii) Financial

The Agreement requires that each side bear its own costs arising from the operation of the Agreement.

(iii) Human Rights

The Agreement provides that its purpose is to ‘advance public safety and security, and to protect privacy, civil liberties and an open Internet.’

The UK has secured assurances that permission must be sought from the UK by US authorities to use data from a UK CSP in a prosecution, in a case where the death penalty is sought.

(iv) Reservations and Declarations

None

(v) Implementation

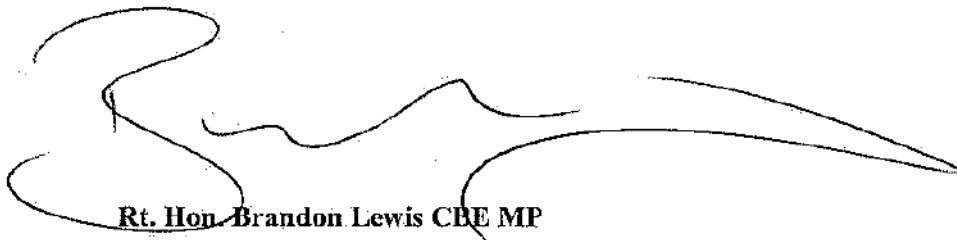
Prior to implementation, the Agreement must be ratified by Parliament and then designated as an international agreement under the Investigatory Powers Act 2016 and Crime (Overseas Production Orders) Act 2019. The relevant Statutory Instrument(s) will therefore need to have been enacted before the Agreement can be brought into force. The US Congress must also ratify the Agreement before it is brought into force.

(vi) Consultation

This Agreement covers international relations between the UK and US which is not a power devolved to the devolved administrations. However, the Agreement does affect

powers which are devolved in that it provides all parts of the UK with the right to make requests under the Agreement, providing they have met the requirements under the Agreement. The scope of the Agreement does not cover the Channel Islands, the Isle of Man or any British Overseas Territories.

HMG have worked closely with industry in both the UK and US on the desirability and practicality of implementing the Agreement, and they have been supportive. HMG officials will continue to engage with them throughout the implementation period.

A handwritten signature in black ink, appearing to read 'Brandon Lewis', written over a faint, illegible stamp or watermark.

Rt. Hon. Brandon Lewis CBE MP

Minister of State for Security and Economic Crime

Home Office