HOUSE OF LORDS Library Briefing

# Crime (Overseas Production Orders) Bill [HL]
# HL Bill 113 of 2017–19


## Summary

The Crime (Overseas Production Orders) Bill [HL] is a government bill introduced in the House of Lords on 27 June 2018. It is scheduled to have its second reading on 11 July 2018.

Electronic information is increasingly important for the investigation and prosecution of criminal offences. The companies that provide services which generate or store this data are often located outside the UK, particularly in the United States. UK law enforcement agencies and prosecutors can request electronic data from overseas for evidential use through the mutual legal assistance treaty (MLAT) process, but such requests can take many months.

The Bill would enable law enforcement agencies and prosecutors to apply through the UK courts for a court order requiring service providers outside the UK to produce or grant access to electronic data for the purposes of investigating and prosecuting serious crimes. Such an order would be known as an 'overseas production order'. An application for an overseas production order could only be granted if a judge was satisfied that the data was likely to be of substantial value to the criminal proceedings or investigation for which it was being requested, and that it would be in the public interest.

Applications for an overseas production order could only be made if there was an international agreement in place between the UK and the territory where the relevant provider was based. To date, no such agreements have been concluded, but the UK has been negotiating a bilateral data-sharing agreement with the United States since 2015. The US passed the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act) in March 2018 which provides authorisation for the US to conclude international agreements through which foreign governments can seek data directly from US companies without each request having to be reviewed by the US Government.

The Government has stated that the Bill would bring into line the powers of the courts to seek access to data stored by companies based in the UK with those based in territories with which the UK has a relevant international agreement.


**Table of Contents**




Nicola Newson
5 July 2018

## Table of Contents



---

## 1. Introduction

The Crime (Overseas Production Orders) Bill [HL] is a government bill that was introduced in the House of Lords on 27 June 2018. It is scheduled to have its second reading on 11 July 2018. The Home Office has produced explanatory notes, a factsheet, an impact assessment and a delegated powers memorandum to accompany the Bill.

The Bill would enable law enforcement agencies and prosecutors to apply through the UK courts for a court order requiring service providers outside the UK to produce or grant access to electronic data for the purposes of investigating and prosecuting serious crimes. Such an order would be known as an 'overseas production order'. Applications could only be made if there was an international agreement in place between the UK and the territory where the relevant provider was based. To date, no such agreements have been concluded, but the UK has been negotiating a bilateral data-sharing agreement with the United States since 2015. An application for an overseas production order could only be granted if the judge was satisfied that the data was likely to be of substantial value to the criminal proceedings or investigation for which it was being requested, and that production of the data would be in the public interest.

The Government has stated that the ability to apply for an overseas production order through the domestic courts would make the process for gaining cross-border access to electronic data faster and more reliable than the current processes which rely on mutual legal assistance treaties.[1] These have been criticised for being too bureaucratic and time-consuming. The Government has stated that the Bill would bring into line the powers of the courts to seek access to data stored by companies based in the UK with those based in territories with which the UK has a relevant international agreement.[2] Electronic data can already be obtained if there are reasonable grounds for believing it is stored on, or accessible from, premises in the UK.[3] While the Investigatory Powers Act 2016 allowed for the acquisition of data from overseas for investigation purposes, it does not apply to the use of such data on an evidential basis.[4]

Provisions in the Bill set out:

- Scope and reach of an overseas production order and who may apply for one.
- Requirements which need to be met before a judge makes an overseas production order and what must be included in the

[1] Home Office, *Crime (Overseas Production Orders) Bill Factsheet*, 28 June 2018.
[2] ibid.
[3] ibid.
[4] ibid.

application for an order.

- Restrictions on serving an overseas production order, including the time period within which the data covered by the overseas production order must be supplied.
- Additional safeguards and protections for certain types of data [such as confidential personal records and confidential journalistic material].
- The ways in which an overseas production order can be served.[5]

## 2. Background

### 2.1 Current Practice: Mutual Legal Assistance Treaties

According to the Home Office, electronic information is increasingly important for the investigation and prosecution of criminal offences.[6] However, the companies that provide services which generate and/or store such data are often located outside the UK, particularly in the US. The Home Office has explained that this puts the data beyond the reach of existing domestic court orders, which either cannot be made when the data is not in or accessible from the UK, or cannot be served extra-territorially.[7]

Paddy McGuinness, the UK's Deputy National Security Adviser on Intelligence, Security and Resilience from 2014 to 2018,[8] explained in an interview how this causes difficulties for UK investigators and prosecutors:

> […] our law enforcement and security agencies tell me that US communication services are used by 90 percent of their suspects and that reflects the broader penetration by the British market by these services. So we can read across from that into the figures for serious and organised crime and terrorism […] In almost every [terrorism] investigation we conduct, those we investigate use services provided by US CSPs [communications service providers].
>
> […] It does not make sense that criminals plotting a major drug deal, a murder, a kidnap, trafficking people or sexually abusing a child in the UK can have their communications intercepted if they communicate via text message, but if they use a US company's services their data should be out of reach of UK law enforcement.[9]

---

[5] Home Office, *Crime (Overseas Production Orders) Bill Factsheet*, 28 June 2018.
[6] Explanatory Notes, p 2.
[7] ibid.
[8] Royal United Services Institute, 'Paddy McGuinness', accessed 4 July 2018; and Richard Kerbaj, 'British Security Chief to Advise Qatar on World Cup Security', *Times* (£), 14 January 2018.
[9] Andrew Keane Woods, 'Interview: The British Perspective on the Cross-Border Data Problem', Lawfare Blog, 7 February 2018.

Currently, when UK authorities are seeking access to data for evidential purposes from providers based overseas, they have to do so using mutual legal assistance channels.[10] Mutual legal assistance treaties (MLATs) are agreements between two or more countries which create obligations under international law for governments to assist one another in criminal investigations and prosecutions.[11] According to Access Now, a digital rights campaign group, there has recently been a "huge growth" in MLAT requests to access online records (such as subscriber details, email content, metadata and social media) from companies such as Google, Facebook, Yahoo and Twitter, which treat the vast majority of their data as being located in California and therefore subject to Californian jurisdiction.[12]

As of 2016, the UK had signed bilateral MLATs with 40 countries—including the US—and was also party to multilateral MLATs through bodies such as the EU and the Council of Europe.[13]

The MLAT system can involve many steps, which means that requests for information or other assistance can take a long time to be processed. For example, incoming MLAT requests to the US are handled as follows:

> When a request for legal assistance is submitted to the United States, OIA [the Office of International Affairs in the Criminal Division of the US Department of Justice] receives and conducts an initial review to ensure that the request contains all necessary information and comports with required formats. OIA then transmit the request to the US Attorney in the jurisdiction where the witness or evidence is located. The US Attorney brings the request before a federal district court by filing a request for a court order or warrant authorising the United States to carry out the action sought by the foreign nation. Before authorizing the action, courts review the request to ensure that it complies with the underlying treaty and US law and constitutional requirements. After a warrant or court order has been issued and the provider transfers the data to the US Government, OIA and the Federal Bureau of Investigation (FBI) review the material in an effort to minimise production of information that is not responsive to the request.
>
> According to the 2013 President's Review Group on Intelligence and Communications Technologies, MLAT requests submitted to the United States take an average of approximately 10 months to complete.[14]

---

[10] Home Office, *Crime (Overseas Production Orders) Bill Factsheet*, 28 June 2018.
[11] Access Now, 'Mutual Legal Assistance Treaties: Frequently Asked Questions', accessed 4 July 2018.
[12] ibid.
[13] Home Office, *International MLA and Extradition Agreements the UK Is Party To*, April 2016.
[14] Stephen P Mulligan, *Cross-Border Data Sharing Under the CLOUD Act*, Congressional Research Service, 23 April 2018, p 14.

The bureaucratic and time-consuming nature of the MLAT process has been criticised by UK officials involved in security and law enforcement. Paddy McGuinness, former Deputy National Security Adviser, said that while MLATs were "important", they were "not the answer to the cross-border data problem":

> These treaties are designed for obtaining evidence after a crime has been committed. Even in those cases, it can sometimes take too long to receive the necessary evidence—up to nine months—in order to progress an investigation and secure convictions. It is widely acknowledged that MLAT processes are too slow for rapidly developing counter-terrorism and serious crime investigations.[15]

Sir David Anderson, the then Independent Reviewer of Terrorism Legislation, concluded in a report in 2015 that "there is little dispute that the MLAT route is currently ineffective", principally because "it is too slow to meet the needs of an investigation, particularly in relation to a dynamic conspiracy".[16] Sir Nigel Sheinwald, who was appointed as the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing in 2014, also noted practical difficulties with the existing MLAT process:

> […] the MLAT process is widely criticised for being slow, unresponsive (it can take up to nine months for information to be returned) and bureaucratic (it currently involves hard copies of legal documents being couriered across the Atlantic through numerous intermediary bodies.[17]

Sir David Anderson and Sir Nigel Sheinwald both recommended that the Government should try to improve the MLAT process, but both were also in favour of the Government developing a new approach. Sir David recommended that, in order to address deficiencies in access to material from overseas service providers, the Government should "take a lead in developing and negotiating a new international framework for data-sharing among like-minded democratic nations".[18] Sir Nigel also called for a new international framework that would allow for easier data-sharing between countries:

> While we should improve our current Mutual Legal Assistance Treaty,

---

[15] Andrew Keane Woods, 'Interview: The British Perspective on the Cross-Border Data Problem', Lawfare Blog, 7 February 2018.
[16] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015, p 215. In June 2018, David Anderson was awarded a knighthood and it was announced that he would receive a life peerage; he has not yet taken his seat in the House of Lords.
[17] Cabinet Office, *Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing—Sir Nigel Sheinwald*, 25 June 2015.
[18] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015, p 295.

> it will never be fast enough or have a scope wide enough to allow for urgent counter-terrorism and similar requests. I have therefore been discussing with the companies and US and other governments a solution that would allow certain democratic countries—with similar values and high standards of oversight, transparency and privacy protection—to gain access to content in serious crime and counter-terrorism cases through direct requests to the companies. This proposal offers a sustainable and longer-term solution to data sharing and would aid in resolving inter-jurisdictional issues.[19]

### 2.2 Future Data Sharing Agreement with the US

The Government has stated that the Bill would address the limits of the MLAT system by creating a new overseas production order with extra-territorial scope.[20] This extra-territorial scope could only be exercised where an overarching international agreement between the UK and another country gave authorisation for overseas production orders made in the UK courts to have effect in the other country. The Government has explained that the Bill has been drafted to reflect "the anticipated future framework required to implement such international agreements or arrangements in future". Currently the only such agreement being negotiated is between the UK and the US, although the UK Government has said it "envisages wider application" of the Bill to other countries in the long term through similar arrangements.[21]

Work on an agreement with the US appears to have been ongoing since 2015. Sir Nigel Sheinwald wrote in June 2015 that his work had "reinforced the need for new longer-term, international arrangements, and more strategic relationships with the companies".[22] He said that relevant government departments would be taking this work forward. In the same month, Theresa May, who was then Home Secretary, said that as a result of Sir Nigel's work, the Government would be "looking at a broader international framework within which the companies [communications service providers and social media platforms] will operate in order to enable access to the data".[23]

In March 2016, at the second reading of the bill that became the Investigatory Powers Act 2016, Mrs May said the Government was in formal negotiations with the United States to take forward Sir Nigel's

---

[19] Cabinet Office, *Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing—Sir Nigel Sheinwald*, 25 June 2015.
[20] Explanatory Notes, p 2.
[21] ibid, and Home Office, *Impact Assessment: Crime (Overseas Production Orders) Bill*, dated 11 May 2018, published 28 June 2018, p 5.
[22] Cabinet Office, *Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing—Sir Nigel Sheinwald*, 25 June 2015.
[23] HC *Hansard*, 11 June 2015, col 1363.

recommendations on a new international framework, and the Investigatory Powers Bill had been drafted to accommodate any such future agreement.[24]

Earl Howe, Minister of State at the Ministry of Defence, provided an update on these negotiations during the Investigatory Powers Bill's passage through the House of Lords. He said that the proposal was for a framework "under which communications service providers based in one country could disclose data directly to the other for serious criminal and counter-terrorism investigations when required to by a valid warrant or order, without facing a conflict of law".[25] He explained that the US Government had sent a legislative proposal to Congress in July 2016 that, if passed, would pave the way for a bilateral agreement between the UK and US Governments. He said the UK Government hoped that such an agreement could be in place as soon as possible, but it would depend on the changes required to US legislation.

Paddy McGuinness, then the UK's Deputy National Security Adviser, gave testimony to the US House of Representatives' Judiciary Committee in June 2017, in which he outlined the UK's hopes for a bilateral agreement with the US on data access. He argued that such an agreement would "recognise the high standards of authorisation and oversight that the UK and US have in place" and would "allow companies based in one country to comply with lawful orders for the contents of electronic communications from the other", specifically to combat serious crimes, including terrorism.[26] He said that major US technology companies were supportive of such an agreement as it would protect them from conflicts of law and enable them to resist calls from countries with lower privacy standards to hand over their data.

Mr McGuinness said that the UK Government was "in full agreement" with the US Department of Justice that a UK-US bilateral data sharing agreement should:

i. Not allow the UK to get data on US nationals or anyone in the US.

ii. Limit access to targeted orders for data (ie a specific individual, phone number, email address or other identifier), and not bulk access to data.

iii. Be limited to prevention, detection, investigation or prosecution of serious crime, including terrorist activity or the proliferation of chemical, biological, radiological or nuclear weapons.

---

[24] HC *Hansard*, 15 March 2016, col 823.
[25] HL *Hansard*, 11 October 2016, col 1847.
[26] United States House Judiciary Committee, *Written Statement of Mr Paddy McGuinness, Deputy National Security Adviser, United Kingdom*, 15 June 2017.

iv. Permit orders for 'surveillance' or 'real-time' access in order to prevent attacks and crimes before they occur.

v. Be 'encryption neutral'. Any Agreement should not include terms on encryption which should continue to be discussed by governments and companies as a separate issue.[27]

Mr McGuinness stated that the UK did not believe such a bilateral agreement would require the UK and the US to have identical legal frameworks, but it was important that there should be "shared high standards of authorisation, transparency, privacy protection and oversight".[28] He said the UK hoped that Congress would pass relevant legislation in the US "as a priority in 2017".

## 2.3 US CLOUD Act

The Clarifying Lawful Overseas Use of Data Act, known as the CLOUD Act, was passed into United States law by the Consolidated Appropriations Act 2018 in March 2018.[29] The CLOUD Act provides authorisation for a new form of international agreement to be concluded by the United States, through which foreign governments can seek data directly from US companies without such requests having to be reviewed individually by the US Government.

Earlier US legislation, the Electronic Communications Privacy Act (ECPA), passed in 1986, prohibited service providers from disclosing the content of electronic communications directly to foreign governments without a statutory exception or a warrant from a US federal court being in place.[30] It thereby functioned as a "blocking statute", so that foreign governments wishing to access data held by US companies would have to do so through the MLAT process, or by making requests via letters rogatory where no MLAT existed.[31] US data-holding companies could find themselves subject to potentially conflicting legal obligations, if they were subject to foreign court orders requiring data to be released but simultaneously prohibited by US law from releasing it to a foreign government.[32]

---

[27] United States House Judiciary Committee, *Written Statement of Mr Paddy McGuinness, Deputy National Security Adviser, United Kingdom*, 15 June 2017.
[28] ibid.
[29] United States Congress, 'Consolidated Appropriations Act 2018', 23 March 2018.
[30] Stephen P Mulligan, *Cross-Border Data Sharing Under the CLOUD Act*, Congressional Research Service, 23 April 2018, p 11.
[31] ibid. A letter rogatory, also known as a letter of request, is a request from a court in one country to the judiciary of a foreign country to perform a specified act that would violate the foreign country's sovereignty if done without its approval (Thomson Reuters Practical Law, 'Glossary: Letter Rogatory', accessed 5 July 2018).
[32] Stephen P Mulligan, *Cross-Border Data Sharing Under the CLOUD Act*, Congressional Research Service, 23 April 2018, p 15.

The CLOUD Act creates a new model for data-sharing between the US and other countries. It authorises the US to conclude executive agreements with other countries which would remove the ECPA restrictions on US companies disclosing data directly to a foreign government in response to orders issued by that country.[33] A briefing by the US Congressional Research Service explains that under the CLOUD Act, when a foreign nation with a CLOUD Act agreement issues an order seeking data from a provider in the US, the provider can deliver the requested data without civil or criminal penalty under ECPA.[34] However, neither the CLOUD Act itself, nor an international agreement made under it, would create a legal obligation for US service providers to comply with a data request from a foreign government. The foreign government would need authority under its own domestic law to issue an order seeking the data.

Section 105 of the CLOUD Act sets out a number of safeguards that would apply to international agreements and to orders made by foreign governments. Before the US could conclude an agreement under the CLOUD Act, the US Attorney General and US Secretary of State would have to make four certifications, namely that:

(1) The domestic law of the foreign government "affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement".
(2) The foreign government had adopted "appropriate procedures" to minimise the acquisition, retention and dissemination of information about US persons
(3) The terms of the agreement would not create an obligation for providers to decrypt data, or create any limitation that prevents providers decrypting data.
(4) Orders made under the agreement would be subject to certain requirements, for instance they:

- could not intentionally target a US person; a person located in the US; or any other person if the purpose was to obtain information about a US person or a person located in the US.
- would have to be for the purpose of obtaining information relating to the prevention, detection or prosecution of serious crimes, including terrorism.
- would have to identify a specific person, account, address or personal device, or some other specific identifier.

[33] Stephen P Mulligan, *Cross-Border Data Sharing Under the CLOUD Act*, Congressional Research Service, 23 April 2018, p 15. The Congressional Research Briefing explains that 'executive agreements' are "binding international agreements entered into by the Executive based on a source of authority other than the Treaty Clause" of the US Constitution.
[34] ibid, p 16.

- would have to be in compliance with the domestic law of that country.
- would have to be based on a reasonable justification based on "articulable and credible facts, particularity, legality and severity regarding the conduct under investigation".
- would have to be subject to review or oversight by a court, judge, magistrate or other independent authority.
- would have to be for a limited and reasonable duration, if the order was for interception of real-time communications.
- could not be used to infringe freedom of speech.

The CLOUD Act also requires that when the US concludes an agreement with another country, that country must allow the US reciprocal rights of data access.[35]

The Congressional Research Service notes that the CLOUD Act has had a mixed reception, with supporters arguing it solves a practical legal problem, and critics expressing concerns about civil liberties and human rights:

> Some argue that the Act provides a practical remedy for problems related to the globalisation of evidence and the increased demand for data stored overseas in criminal cases. Supporters assert that the need for data stored abroad, which often is held by US internet companies, has overburdened the legal architecture established in the MLAT and letters rogatory systems, rendering those systems "outdated and inefficient". Supporters also argue that the CLOUD Act provides adequate protection for privacy, civil liberties, and human rights […] Several major US technology companies—including Apple, Facebook, Google, Microsoft, and Oath—support the legislation, calling it an effective legislative solution that reduces conflicts of laws.
>
> Critics of the CLOUD Act argue that it poses a threat to civil liberties and human rights by lowering the standards previously necessary to obtain evidence in cross-border criminal investigations and prosecutions. They contend that the CLOUD Act's standard for individualized suspicion—"reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation"—is vague and may not rise to the level of probable cause necessary to obtain a judicial warrant under US law. Some argue that the executive branch's decision to certify a country as satisfying the CLOUD Act's standards should be subject to judicial or other review. Others contend that the concept that foreign nations' data requests do not need individualised review if the nations'

[35] Stephen P Mulligan, *Cross-Border Data Sharing Under the CLOUD Act*, Congressional Research Service, 23 April 2018, p 18.

> domestic laws meet the Act's eligibility criteria is flawed because foreign governments' real-world operations may not comport with their domestic laws and may change over time […] Others contend, among other things, that the law should increase the requirements for foreign government to obtain access to real-time communications to the same standards that apply to the United States' interception of live communications in the Wiretap Act.[36]

In a phone call with President Trump in February 2018, the Prime Minister, Theresa May, "stressed the great importance of the legislation to the UK authorities in investigating criminal and terrorist activity in the UK".[37] Mrs May and Mr Trump "agreed the passage of the Act through the US legislative system was vital for our collective security".

The UK Government has stated that the US passed the CLOUD Act "in anticipation and preparation" for a bilateral UK-US data access agreement, "enabling the US legislative change required to give effect to this agreement".[38] The UK Government described the Crime (Overseas Production Orders) Bill as "the final element of legislative change required to enable UK law enforcement to take advantage of the proposed agreement when investigating and prosecuting crime".[39] In a document written in May 2018 and published in June 2018, the UK Government said that the agreement itself was "still being finalised".[40]

### 2.4 European Production Orders

Separately from the CLOUD Act and the Crime (Overseas Production Orders) Bill, the European Commission published proposals in April 2018 for EU legislation to create a European Production Order as part of a package of measures on electronic evidence.[41] The proposed European Production Order would allow a judicial authority in one EU member state to request electronic evidence (such as emails, texts or messages in apps) directly from a service provider offering services in the EU and established or represented in another member state, regardless of the location of data, which would be obliged to respond within ten days, and within six hours in cases of emergency (as compared to 120 days for the existing European Investigation Order or ten months for a Mutual Legal Assistance procedure). The European Commission said that this proposal would "make it easier and

---

[36] Stephen P Mulligan, *Cross-Border Data Sharing Under the CLOUD Act*, Congressional Research Service, 23 April 2018, pp 21–2.
[37] Prime Minister's Office, 'PM Call with President Trump: 6 February 2018', 6 February 2018.
[38] Home Office, *Impact Assessment: Crime (Overseas Production Orders) Bill*, dated 11 May 2018, published 28 June 2018, p 4.
[39] ibid, pp 4–5.
[40] ibid, p 5.
[41] European Commission, 'Security Union: Commission Facilitates Access to Electronic Evidence', 17 April 2018.

faster for police and judicial authorities to obtain the electronic evidence, such as emails and documents located on the cloud, they need to investigate, prosecute and convict criminals and terrorists".[42]

As the Regulation would be a justice and home affairs (JHA) measure, the UK would be able to decide whether to opt in. As of May 2018, the Government expected it would have to take this decision by August 2018.[43] The Government explained the factors it would consider when deciding whether to opt in:

> Our approach to this work stream previously has been to caution against EU legislation, given there are existing tools both within the EU and being developed internationally to tackle similar issues.
>
> We will examine any benefits to the UK in participating in this measure, and in particular whether it would provide the UK with additional tools to support criminal investigations, whether it could provide for greater access to data beyond what our domestic capabilities offer, including through evaluating this measure against existing tools such as the EIO [European Investigation Order] and MLA [mutual legal assistance]. In addition, we will assess the likely level of usage of the new system by UK law enforcement agencies.[44]

The House of Commons European Scrutiny Committee noted that under the terms of the draft Withdrawal Agreement, if the proposed Regulation was adopted after 29 March 2019, there was a possibility it might not apply to the UK during the transition/implementation period, even if the UK had decided before exit day to opt in to the measure.[45] The Committee sought clarification from the Government about whether the Regulation would apply to the UK during the transition period depending on different possible timings for the date on which the Regulation ended up being adopted or taking effect.[46] The Committee called for further information on the Government's evaluation of existing tools and mechanisms—domestic, EU or international—for obtaining electronic evidence stored in a different jurisdiction.[47] The Committee also indicated it would welcome further information on the progress made in negotiating a UK-US data agreement, its main provisions, and how UK participation in the proposed Regulation

---

[42] European Commission, 'Security Union: Commission Facilitates Access to Electronic Evidence', 17 April 2018.
[43] Home Office, *Explanatory Memorandum on Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence*, 3 May 2018, para 16.
[44] ibid, paras 24–5.
[45] House of Commons European Scrutiny Committee, *Twenty-Eighth Report of Session 2017–19*, 22 May 2018, HC 301-xxvii of session 2017–19, p 9.
[46] ibid, p 22.
[47] ibid, p 20.

might affect the operation of the agreement.[48]

## 3. Bill Provisions

### 3.1 Overseas Production Orders (Clauses 1 and 15)

Clause 1 would enable a judge to make an 'overseas production order' on an application from an 'appropriate officer' (as defined in clause 2). An overseas production order would be an order which would require the person against whom the order was made to produce or give access to specified electronic data (clause 1(4)).

Clause 1 would provide that a judge could make an overseas production order only if:

- each of the requirements specified in clause 4 for making the order was fulfilled;
- the application specified the designated international cooperation arrangement under which the application was being made;
- the application gave details of the electronic data being sought; and
- the application did not seek data which the applicant had reasonable grounds to believe was 'excepted electronic data' (as defined in clause 3).

Clause 15 would enable a judge advocate to make an overseas production order on application from a member of a service police force. Judge advocates are judicial office-holders who preside in the courts that operate within the Service Justice System.[49] 'Service police force' is a term used to describe collectively or individually the Royal Military Police, the Royal Navy Police and the Royal Airforce Police.[50] The judge advocate would have to be satisfied that all the requirements in clause 4 were met before s/he could make an overseas production order.

### 3.2 Designated International Cooperation Arrangements (Clause 1)

Clause 1(5) would allow the Secretary of State to make regulations designating an international agreement as one in relation to which overseas production orders could be made. The Home Office has explained that this

[48] House of Commons European Scrutiny Committee, *Twenty-Eighth Report of Session 2017–19*, 22 May 2018, HC 301-xxvii of session 2017–19, p 21.
[49] Courts and Tribunals Judiciary, 'Judge Advocate General', accessed 4 July 2018.
[50] Her Majesty's Inspectorate of Constabulary, *An Inspection of the Leadership of the Royal Military Police in relation to its Investigation*, July 2015, p 17.

power would enable the Government to give domestic legal effect to international agreements.[51] The Home Office has suggested that "the UK may enter into a number of such arrangements in future", and that it would therefore be appropriate for the designation to be done through secondary legislation, rather than requiring primary legislation for each new international agreement.

The Home Office has noted that "most international agreements entered into" would be subject to the parliamentary procedures for scrutinising treaties set out in the Constitutional Reform and Governance Act 2010, and it therefore argues that the regulations to designate an international agreement under the Bill should be made by the negative procedure, as Parliament would already have had the opportunity to scrutinise the international agreement itself.[52]

### 3.3 Appropriate Officers (Clause 2)

Clause 2 sets out who would qualify as an 'appropriate officer' who could make an application to the court for an overseas production officer. In England, Wales and Northern Ireland, the following would be deemed as appropriate officers:

- A constable
- A Revenue and Customs officer
- A member of the Serious Fraud Office
- An accredited financial investigator (only for the purposes of a confiscation investigation or money-laundering investigation)
- A counter-terrorism financial investigator (only for the purposes of either a terrorist investigation relating to terrorist property, or a terrorist financing investigation, depending on which provisions of the Terrorism Act 2000 the investigator had been appointed under)
- A person appointed by the Financial Conduct Authority under section 168(3) or (5) of the Financial Services and Markets Act 2000 to conduct an investigation.

In Scotland, the following would be deemed as appropriate officers:

- A procurator fiscal
- If authorised by a procurator fiscal to carry out functions under

[51] Home Office, *Crime (Overseas Production Orders) Bill Delegated Powers Memorandum*, 26 June 2018, p 2.
[52] For further information about the procedures under the Constitutional Reform and Governance Act 2010, see: House of Commons Library, *Parliament's Role in Ratifying Treaties*, 17 February 2017.

this legislation:

- A constable
- A Revenue and Customs officer
- A person appointed by the Financial Conduct Authority under section 168(3) or (5) of the Financial Services and Markets Act 2000 to conduct an investigation

The Secretary of State could make regulations under clause 2 using the negative procedure to add other categories of people to the list of appropriate officers. In the case of Scotland, this could only be done after consultation with Scottish Ministers (clause 16(3)), and any new categories of person added to the list could only act as appropriate officers with authorisation from a procurator fiscal. The Home Office has suggested that the list of appropriate officers might need to be updated to reflect changing circumstances in light of any future international agreements.[53]

### 3.4 Electronic Data and Excepted Electronic Data (Clause 3)

Clause 3 specifies that 'electronic data' for which an overseas production order could be made means "data stored electronically". However, an overseas production order could not be made in respect of 'excepted electronic data', defined in clause 3 as data that is:

- Subject to legal privilege; or
- A confidential personal record, namely a confidential record concerning an identifiable individual, living or dead, and relating to their physical or mental health, spiritual counselling or assistance given to them, or other counselling or assistance given to them for the purposes of their personal welfare. The explanatory notes to the Bill give medical records as an example of confidential personal records that would be exempt from overseas production orders.[54]

Confidential personal records would not be counted as excepted electronic data for the purposes of a terrorist investigation; however, they would still be classed as excepted electronic data for the purposes of a terrorist financing investigation (clause 3(5)).

Clause 3(4) provides that if the overseas production order was against a telecommunications provider, then communications data (which the explanatory notes describe as "data relating to the communication rather

[53] Home Office, *Crime (Overseas Production Orders) Bill Delegated Powers Memorandum*, 26 June 2018, p 4.
[54] Explanatory Notes, p 4.

than its content") would be treated as excepted electronic data.[55]

### 3.5 Requirements for Making an Order (Clause 4)

Clause 4 sets out a series of requirements that would have to be fulfilled for a judge to make an overseas protection order. The judge would have to be satisfied that there were reasonable grounds for believing all the following:

- The person against whom the order is sought operates in, or is based in, a country or territory outside the UK covered by the designated international cooperation specified in the application.
- An indictable offence has been committed and legal proceedings have begun or an investigation is underway. However, this requirement would not apply if the judge was satisfied that the order was sought for the purposes of a terrorist investigation. The explanatory notes state that this reflects the criteria under which production orders may already be sought against those in the UK.[56]
- The person against whom the order is sought has some or all of the data covered by the application.
- The data is "likely to be of substantial value (whether or not by itself)" to the legal proceedings or investigation.
- It is in the public interest for the data to be made available, having regard to the likely benefit to the proceedings or investigation, and to the circumstances in which the person against whom the order is sought has possession or control of the data.

Clause 4(1)(b) would give the Secretary of State the power to make regulations to create additional requirements that would have to be met before an application could be granted. Any regulations made under this power would be subject to the affirmative procedure (clause 16(4)). The Home Office has noted that future international cooperation arrangements might contain additional terms or requirements that would need to be reflected in domestic legislation.[57]

### 3.6 Contents and Effect of Order (Clauses 5, 6 and 8)

Clause 5 sets out what a judge would need to specify in the order, once s/he was satisfied that the application met the required criteria. The judge could make an order covering only some of the electronic data sought in the

---

[55] Explanatory Notes, p 4.
[56] ibid, p 5.
[57] Home Office, *Crime (Overseas Production Orders) Bill Delegated Powers Memorandum*, 26 June 2018, p 5.

application if parts of the application did not meet the required criteria, in particular if it did not meet the 'substantial value' and 'public interest' tests. The judge could not make an order requiring data to be made available if s/he had reasonable grounds for believing that the data fell under the category of 'excepted electronic data'.

When making the order, the judge would have to specify:

- To whom the electronic data must be given; and
- A deadline by when the data must be made available. By default, this would be seven days, but a judge could specify a shorter or longer period if s/he considered it appropriate.

Clause 8 would allow a judge making an overseas production order to include a non-disclosure requirement in the order. This would mean that the person against whom the order was made could not disclose the existence or contents of the order unless they had leave from the judge or written permission from the appropriate officer who applied for the order (or an equivalent appropriate officer) to do so. The order would have to state how long the non-disclosure requirement would last. The explanatory notes to the Bill observe that "the continuation of a non-disclosure requirement is unlikely to be appropriate once the investigation has concluded or proceedings instituted have been concluded".[58] Clause 8 would allow a judge revoking an overseas production order to order that a non-disclosure requirement should continue to apply. The explanatory notes suggest that this may be appropriate if it was clear to the judge that a further overseas production order may be sought.[59]

Clause 6 would create a requirement for the electronic data to be produced, or for access to be granted to the electronic data, in a form in which it could be taken away, and in which it was—or could readily be made—visible and legible.

Clause 6 also specifies that a requirement to produce or give access to electronic data would apply regardless of where the data was stored. This clause further specifies that a requirement to produce or give access to the data would have effect in spite of any other restrictions on the disclosure of information. However, clause 6 clarifies that the person being served with an overseas production order would not be required to produce or give access to any excepted electronic data.

[58] Explanatory Notes, p 6.
[59] ibid.

### 3.7 Variation or Revocation of Order (Clause 7)

Clause 7 would enable a judge to vary or revoke an overseas production order on the application of:

- The appropriate officer who applied for the order, or an equivalent appropriate officer
- Any person affected by the order
- The Secretary of State (in respect of England and Wales and Northern Ireland)
- The Lord Advocate or a procurator fiscal (in respect of Scotland)

An application to vary an overseas production order could be made to seek data not covered by the original order, but this could not include excepted electronic data. A judge could grant an application to vary an overseas production order only if the requirements set out in clause 4 continued to be met.

### 3.8 Service of Order (Clauses 9 and 14)

Clause 9 provides that if an overseas production order was not served within three months of being made, then it would expire. It also provides that only the Secretary of State (in respect of England and Wales and Northern Ireland) and the Lord Advocate (in respect of Scotland) could serve an overseas production order, and they could only do so if they considered that it would be in accordance with a designated international cooperation agreement.

Clause 14 makes provision about the means of serving an overseas production order, as well as serving a notice of application (see clauses 12 and 13) and any other documents relating to UK legal proceedings pertaining to overseas production orders. It would enable an order, notice or other document to be served:

- by any means permitted by rules of court, including electronically (for example, by email)
- on a person located outside the UK:
    - by delivering it to their principal office, business premises or nominated address in the UK
    - by making it available for inspection in the UK, but only if no other means of delivery is reasonably practicable, and only if appropriate steps are taken to bring it to the attention of the person on whom the order, notice or document is being served, as soon as reasonably practicable

- in accordance with arrangements made with the Secretary of State (in England and Wales and Northern Ireland) or the Lord Advocate (in Scotland)

The Home Office has explained that the Bill proposes to retain a discretion for the Secretary of State and the Lord Advocate to make arrangements for the service of an overseas production order depending on the provisions of particular international cooperation arrangements that may be made in future.[60] For example, there might be an agreement that consular staff may serve the order by hand, or that local service agents would be engaged on behalf of the Secretary of State or the Lord Advocate to make arrangements for serving an overseas production order in a particular case.

### 3.9 Retention of Electronic Data and Use as Evidence (Clause 10)

Clause 10 specifies that electronic data produced in compliance with an overseas production order could be kept "for as long as is necessary in all the circumstances". This would include retaining it for use as evidence in legal proceedings relating to a criminal offence. Clause 10 makes consequential amendments to existing legislation (the Criminal Justice Act 2003 and the Criminal Justice (Evidence) (Northern Ireland) Order 2004) to ensure that electronic data obtained through an overseas production order would be admissible as evidence.

### 3.10 Court Procedure (Clause 11)

Under clause 11, rules of court may be used to make provision about what practice and procedure should be followed for court proceedings relating to an overseas production order. Clause 11 also specifies that any orders made under this legislation by a judge in England, Wales or Northern Ireland would have the effect of a Crown Court order. The explanatory notes point out that non-compliance with an overseas production order made by any UK judge (including in Scotland) could give rise to contempt of court proceedings.[61]

### 3.11 Notice of Application (Clauses 12 and 13)

Clause 12 provides that if there were reasonable grounds for believing that the electronic data sought included 'confidential journalistic data', then the application for the overseas production order must be made 'on notice'. Clause 12 defines 'confidential journalistic data' as data which:

- was created or acquired for the purposes of journalism;

---

[60] Home Office, *Crime (Overseas Production Orders) Bill Delegated Powers Memorandum*, 26 June 2018, p 7.
[61] Explanatory Notes, p 7.

- is stored by/on behalf of the person who created or acquired the data for the purposes of journalism; and
- was not created or acquired or intended to be used for furthering a criminal purpose

and

- was created or acquired in circumstances which gave rise to an obligation of confidentiality, and that obligation continues; or
- is subject to a restriction on disclosure, or an obligation of secrecy, contained in any enactment.

The Home Office has stated in the explanatory notes that the requirement to give notice of an application relating to confidential journalistic data would enable a journalist whose material was being sought to be party to the court proceedings considering the application.[62] The explanatory notes also state that it would be for the judge to determine who should be put on notice of such applications, and that rules of court would set out the mechanisms for doing so.

Under clause 13, if a person is served with notice that an application had been made for an overseas production order against them, that person must not conceal, destroy, alter or dispose of any of the data being sought, nor disclose the existence or contents of the application to anybody, unless they had leave from the judge or written permission from the appropriate officer making the application to do so. This would apply to journalists who had been given notice of an application under clause 12, but also to anybody else who had received notice of an application.

If an application did not result in an overseas production order being made, the person who had been served notice would no longer be bound to protect the data or not to disclose the application, unless the judge ordered otherwise.

If an overseas production order was made, the person who had been served notice would no longer be bound to protect the data once the order was served, or if the order ceased to have effect through revocation, expiry after three months without being served, or because it was quashed. The non-disclosure duty would cease to apply to a person given notice once the order was served, unless the order itself contained a non-disclosure requirement.

The Home Office has stated that the aim of this provision is to protect evidence, and prevent prejudice to an investigation, whilst providing the

[62] Explanatory Notes, p 7.

opportunity for affected parties to participate in court proceedings considering access to such material.[63]

### 3.12 General Provisions (Clauses 16 to 20)

Clause 16 makes provision for regulation-making powers under the Bill. Any regulations that added to the list of requirements to be satisfied before a judge could make an overseas production order (clause 4) would have to be made using the affirmative procedure, but all other regulations would be subject to the negative procedure.

Clause 17 points to whereabouts in the Bill definitions can be found for the terms 'appropriate officer', 'designated international cooperation agreement', 'electronic data', 'excepted electronic data', 'judge' and 'overseas production order'.

Clause 18 sets out the territorial extent of the Bill. The Bill would extend to the whole of the United Kingdom, except that clause 10(2) would extend to England and Wales only and clause 10(3) would extend to Northern Ireland only. These are the sub-clauses that make consequential amendments to existing legislation to ensure that data obtained by means of an overseas production order would be admissible as evidence in court.

The Home Office has stated that the Bill relates to matters within the legislative competence of the Scottish Parliament and Northern Ireland Assembly as it provides for a means for devolved law enforcement officers to seek electronic data evidence not covered by specific reservations in relation to a wide range of serious offences, some of which are not reserved/excepted.[64] The Government is seeking the legislative consent of the Scottish Parliament in relation to the Bill; separate commencement provisions exist within the Bill so that the Northern Ireland Executive may consider the application of these powers once it is restored.[65]

Clause 19 contains the Bill's commencement provisions. Clauses 16 to 20 would come into force on the day on which the Bill was passed; the remaining clauses would be brought into force by the Secretary of State by regulations.

Clause 20 sets out the Bill's short title.

---

[63] Explanatory Notes, p 7.
[64] ibid, p 3.
[65] ibid.