HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 8449, 30 November 2018

Crime (Overseas Production Orders) Bill

By Joanna Dawson

Contents:

Contents

Summary

The *Crime (Overseas Production Orders) Bill [HL]* was introduced in the House of Lords on 27 June 2018. It had its third reading on 20 November and is due to have second reading in the House of Commons on 3 December.

The Bill would create a framework to enable law enforcement agencies and prosecutors to apply to a UK court for an 'overseas production order' requiring a person (in practice, generally a communications service provider or 'CSP') in a foreign jurisdiction to produce or grant access to electronic data for the purposes of investigating and prosecuting serious crime. An application would only be granted if the judge was satisfied that the data was likely to be of substantial value to the criminal proceedings or investigations for which it was sought, and that it would be in the public interest.

Overseas production orders would only be available where there was a designated international agreement in place between the UK and the country or territory where the CSP was based. No such agreements are currently in force, but the UK has been in the process of negotiating a data sharing agreement with the USA since 2015.

In March 2018 the US passed the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act), which provides authorisation for a form of international agreement to be concluded by the US, allowing foreign governments to seek data directly from US companies without going through political channels.

The Government has stated that the Bill is required due to the increasing use of software applications over public networks to facilitate criminal activities. Evidence generated by such activity is crucial for investigations into serious crimes, including terrorism. However, the companies holding the data are largely situated outside the UK and therefore beyond the reach of existing domestic production orders.

The Bill received broad support in the House of Lords, but was amended to ensure sufficient parliamentary scrutiny of future international cooperation agreements, and to provide safeguards against UK service providers being required to produce evidence in cases in which the death penalty may be imposed.

1. Introduction

The *Crime (Overseas Production Orders) Bill* was introduced in the House of Lords on 27 June 2018. It was considered by Grand Committee in two sittings and had its third reading on 20 November. Second reading in the House of Commons is scheduled for 3 December.

The Home Office has produced explanatory notes, a factsheet, an impact assessment and a delegated powers memorandum to accompany the Bill.

The Bill would allow law enforcement agencies and prosecutors to apply to a court in the UK for an overseas production order (OPO), which would require an overseas service provider to provide or allow access to stored electronic data specified in the order, for the purposes of investigating or prosecuting serious crime.

OPOs would only be available if there is a designated international cooperation agreement in place between the UK and the territory in which the data is held.

According to the Home Office, the new powers would supplement existing production order powers available under the *Police and Criminal Evidence Act 1984*, the *Terrorism Act 2000*, and the *Proceeds of Crime Act 2002*, which provide for access to data located in the UK.

OPOs would make the process for gaining access to electronic data stored in other jurisdictions faster and more reliable than the current processes, which rely on mutual legal assistance treaties (MLAT). MLA processes have been criticised as slow and bureaucratic, and delays can cause problems with criminal investigations and prosecutions.

The provisions of the Bill would extend across the whole of the UK.

1.1 Mutual Legal Assistance

Currently, when UK authorities are seeking access to data for evidential purposes from providers based overseas, they have to use MLA channels. MLAT are agreements between two or more countries which create obligations under international law for governments to assist one another in criminal investigations and prosecutions.

According to the Home Office, as of 2016 the UK was party to 40 bilateral MLA agreements. There is also an EU MLA Convention which extends to Norway and Iceland.[1]

The UK has an existing MLA agreement with the US. However, the bureaucratic and time consuming nature of the process has been widely criticised.

Lord David Anderson, then Independent Reviewer of Terrorism Legislation, stated in a report in 2015 that

[1] Home Office, *International MLA & Extradition Agreements the UK is party to*, April 2016 [accessed 30 November 2018]

> […] there is little dispute that the MLAT route is currently ineffective. Principally this is because it is too slow to meet the needs of an investigation, particularly in relation to a dynamic conspiracy. For example a request to the United States might typically take nine months to produce what is sought.[2]

He consequently recommended that the Government should seek to address deficiencies in access to material from overseas service providers by "[taking] a lead in developing and negotiating a new international framework for data-sharing among like-minded democratic nations."[3]

Sir Nigel Sheinwald, who was appointed as the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing in 2014, expressed a similar view, recommending improvements to the MLAT process with the US as well as a new international framework:

> MLATs are essential tools for the law enforcement community, primarily in order to obtain information to an evidential standard from other jurisdictions. However, 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). We have suggested a series of practical reforms to our existing MLAT with the United States including standardisation of processes, training and improved guidance.
>
> ….
>
> While we should improve our current Mutual Legal Assistance Treaty, 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 the 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 interjurisdictional issues. This does not undermine the case for updated powers, or greater oversight, which can be taken forward in parallel.[4]

1.2 Data exchange with the USA

The Impact Assessment states that the UK and the US recognise that through legislative changes in both countries, a bilateral Data Access Agreement could enable electronic data to be to be provided in a more efficient and timely manner than under existing MLA arrangements. It states that such an agreement is still being finalised, but that in anticipation and preparation for it, the US passed its CLOUD Act in March 2018, enabling the US legislative change required to give effect to this agreement.[5]

---

2 David Anderson, *A Question of Trust*, June 2015, para 11.26
3 Ibid, page 289
4 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
5 For further detail on the CLOUD Act, see Crime (Overseas Production Orders) Bill [HL], House of Lords Library Briefing, 5 July 2018

Work on this agreement appears to have begun following the conclusion of Sir Nigel Sheinwald's work in 2015.

In 2015, Theresa May, then Home Secretary said "we will be taking Sir Nigel's advice, including pursuing a strengthened UK-US mutual legal assistance treaty process and a new international framework".[6]

According to the Lords Library Briefing on the Bill, 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. 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:

- Not allow the UK to get data on US nationals or anyone in the US.
- Limit access to targeted orders for data (ie a specific individual, phone number, email address or other identifier), and not bulk access to data.
- Be limited to prevention, detection, investigation or prosecution of serious crime, including terrorist activity or the proliferation of chemical, biological, radiological or nuclear weapons.
- Permit orders for 'surveillance' or 'real-time' access in order to prevent attacks and crimes before they occur.
- 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.

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". He said the UK hoped that Congress would pass relevant legislation in the US "as a priority in 2017".[7]

6 HC Deb 11 June 2015, c 1362
7 Crime (Overseas Production Orders) Bill [HL], House of Lords Library Briefing, 5 July 2018

1.3 European Production Order

In April 2018 the European Commission published proposals for EU legislation to create a European Production Order as part of a package of measures on electronic evidence.[8]

This would allow a judicial authority in one EU member state to request electronic evidence directly from a service provider in another member state, regardless of the location of data. The service provider would be obliged to respond within 10 days, and within six hours in cases of emergency.

The Government has decided not to opt in to this measure. In a letter to the European Scrutiny Committee on 28 September, the Minister for Policing and the Fire Service, Nick Hurd said of the proposals

> […] it is not clear how new EU legislation will be a practical way to address the global issue of providing lawful access to data held anywhere in the world, even outside the EU's jurisdiction.[9]

8 European Commission, 'Security Union: Commission Facilitates Access to Electronic Evidence', 17 April 2018.

9 Documents considered by the Committee on 17 October 2018, Law enforcement access to electronic equipment

2. Debate in the House of Lords

2.1 Second reading

Baroness Williams introduced the Bill at second reading, explaining the inadequacies of the MLA process:

> Where evidence is held outside the UK, we must rely on our international partners to help. We must use mutual legal assistance channels—a form of judicial co-operation between states that allows law enforcement officers and prosecutors to obtain evidence from a foreign jurisdiction via the authorities in that jurisdiction. However, the mutual legal assistance process can be slow, and in some cases it may not be timely enough to support an investigation or a prosecution. It requires a formal request to be made to another country, which then assesses it to consider whether it can comply. That country may require a court order or warrant from its own courts to obtain the evidence. This is usually the case for stored electronic data. It would then serve that order or warrant on the service provider in its territory. This process takes time and in some cases might result in delayed or abandoned investigations or prosecutions. It can also delay people being eliminated from a criminal investigation.[10]

She suggested that the Bill's provisions reflected the UK's "existing high levels of privacy protection, respect for freedom of speech and international human rights law", and that UK law enforcement officers will be obliged to deal with any data they receive under an overseas production order in accordance with existing protections under the *Data Protection Act 2018*. [11]

The Bill was broadly welcomed by the opposition parties. However, Lord Paddick raised a number of concerns on behalf of the Liberal Democrats, including whether or not the Bill would affect the UK's ability to obtain a data protection adequacy agreement as a third party outside of the EU, and whether the Bill makes sufficient provision for the enforcement of OPOs.[12]

Lord Rosser raised concerns about compliance with the European Convention on Human Rights, and about the production of evidence in death penalty cases, on behalf of Labour.[13]

2.2 Debate and amendments

In committee the debate focused on a number of issues, in particular:

- Human rights compliance and the death penalty;
- Transparency and parliamentary scrutiny of future international cooperation agreements;
- Excepted data and additional safeguards for journalistic material;
- Enforcement of OPOs;

---

10 HL Deb 11 July 2018, c919
11 Ibid c290
12 Ibid C922
13 Ibid C924-927

- Data protection and adequacy

The Government tabled amendments at report stage which sought to address concerns about parliamentary scrutiny of future treaties to which the Bill would apply. Amendment 4, would amend clause 1 to provide that a designated international cooperation arrangement must be a "relevant treaty", meaning that it is one that has been laid before Parliament under section 20(1)(a) of the *Constitutional Reform and Governance Act 2010*. Baroness Williams explained the effect of the amendment:

> The effect of the amendment would be to ensure that where the Secretary of State, by way of regulations, wishes to designate an arrangement under the Bill, they can do so only if that arrangement is a treaty that has been laid before Parliament for scrutiny under CRaG. Only treaties that have been laid before Parliament under CRaG can be designated. However, it is still possible for an agreement to be designated before ratification. There may be operational reasons why one would want to designate an agreement before ratification has been finalised. For example, an agreement may come into force on ratification—depending on the terms of the agreement—in which case designating after ratification may be too late and there may be a risk of breach of obligations under the agreement.[14]

Amendment 4 was agreed.

Labour tabled an amendment to clause 1 which would provide that in any agreement on overseas production orders and the provision of electronic data under the terms of the Bill, assurances must be obtained from the other country concerned, that the death penalty will not be applied. Lord Rosser explained the amendment:

> An order from this country for an overseas production order applying to a service provider in the USA would, under the Bill, be made in a UK court. The service provider in the USA would, under the terms of the arrangements likely to be concluded, be expected to comply. In fact, as I understand it again, our Government have stated that they will not seek such an order unless they know that the provider would be willing to comply voluntarily.
>
> As understand it again, service providers are likely to be willing to comply because the Bill will provide them with legal protection for releasing such electronic data. Likewise a service provider in this country would, in the normal course of events, be expected to comply with an overseas production order made by a court in another country—such as America, with which it looks as though we are close to concluding an agreement—under the terms of the Bill. I am not sure that there has been an indication from the American authorities that they would seek such an order only if they knew that the relevant service provider over here would comply, so some form of enforcement action could be the result if there was non-compliance.
>
> Our concern in respect of the death penalty, to which this amendment relates, is that in a number of states in the USA it can be handed down as the sentence if a defendant is found guilty of certain serious crimes, including acts of terrorism. In the UK we are opposed to the death penalty—government Ministers have

[14] HL Deb 22 October 2018, c671

> repeatedly stated that—and do not apply it as a sentence. However an overseas production order made by a court in the USA for electronic data from a service provider in this country could result in a situation whereby that electronic data might be significant in or key to enabling a court in America to convict a defendant who could be a citizen of any country, including Britain, of an offence carrying the death penalty as a possible sentence.[15]

The Government sought to resist the amendment, arguing that whilst the objective was to obtain a satisfactory death penalty assurance, seeking to do so in this way might jeopardise the ongoing negotiations with the US. Baroness Williams further committed to bring forward an amendment in the Commons which would:

> […] not pre-empt negotiations with the US, or any future agreement with another country, but would instead absolutely guarantee that Parliament has the chance to conduct proper, thorough scrutiny of relevant agreements and death penalty assurances.
>
> The amendment I envisage would ensure that Ministers cannot make regulations to designate any agreement with a country which retains the death penalty for incoming requests without first laying before Parliament the agreement and details of any assurances obtained. There would then be a defined period during which Parliament would have a chance to examine those details, and this could include scrutiny by any relevant committees.
>
> Finally, the Secretary of State would be obliged to consider any recommendations made by a committee in relation to the assurances before laying regulations to designate the agreement. Of course, the regulations themselves would then be subject to the usual process of parliamentary scrutiny, during which time Members of both Houses could consider any recommendations and respond to them.
>
> Ultimately, it is right that Parliament has a say on the difficult decision between not concluding negotiations on agreements and securing the death penalty assurances we would like. Both the amendments tabled by Labour and Liberal Democrat Peers could lead to our being unable to conclude a data access agreement with the US. If we find ourselves in that situation, law enforcement agencies and the UK intelligence community will continue to be denied timely access to valuable evidence and intelligence.[16]

The House divided and the amendment was agreed.

---

15 HL Deb 22 October 2018, c659
16 Ibid, c663

3. The Bill

The following described some of the key substantive provisions of the Bill. For a full description of each clause, please see the explanatory notes.

3.1 Overseas production orders

Clause 1 would provide for a judge to make an overseas production order on application by an "appropriate officer", provided certain requirements are fulfilled, namely:

- The application must specify:
  - the designated international co-operation arrangement under which the application is made; and
  - the electronic data that is sought;
- The application must not seek "excepted data", as defined by clause 3;

Clause 15 makes equivalent provision for service police to make an application to a judge advocate.[17]

3.2 Designated international cooperation agreements

Clause 1(5) provides that the Secretary of State is precluded from making a designation under section 52 of the Investigatory Powers Act 2016 with respect to an agreement that provides for requests to be made by the authorities of a country or territory which retains the death penalty. Subsection (6) provides that subsection (5) does not apply if the country or territory in question has given assurances that the death penalty will not be applied in the case for which the evidence in question is sought. These provisions are the result of a non-Government amendment at Report stage in the House of Lords. They are intended to reflect the reciprocal nature of the international cooperation agreements envisaged by the Bill, and to preclude the possibility of a UK service provider being required to provide evidence in a case in which the death penalty might be applied.

Clause 1(7) 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 power would enable the Government to give domestic legal effect to international agreements. As the UK may enter into multiple agreements in the future, the delegated power is necessary to avoid the need for primary legislation in each case.

Clause 1(8) defines a relevant treaty for the purposes of subsection (7) as one which has been laid before Parliament under s20(1)(a) of the *Constitutional Reform and Governance Act 2010*. This was added by a

[17] Judge advocates are judicial office-holders who preside in the courts that operate within the Service Justice System.

Government amendment in the House of Lords in order to address concerns regarding parliamentary scrutiny of future agreements.

3.3 Appropriate officers

Clause 2 sets out who would qualify as an 'appropriate officer' for the purposes of making an application under clause 1, namely:

- In England and Wales
  - A constable
  - A Revenue and Customs officer
  - A member of the Serious Fraud Office
  - An accredited financial investigator (for the purposes of a confiscation investigation or money-laundering investigation)
  - A counter-terrorism financial investigator (for the purposes of a terrorist investigation relating to terrorist property, or a terrorist financing investigation)
  - A person appointed by the Financial Conduct Authority (FCA) under section 168(3) or (5) of the Financial Service and Markets Act 2000
- In Scotland
  - A procurator fiscal
  - If authorised by a procurator fiscal, a constable; a Revenue and Customs Officer; a person appointed by the FCA, as above

3.4 Excepted electronic data

Clause 3 defines excepted electronic data for the purposes of clause 1, in respect of which an application for an OPO may not be sought. This is data which is subject to legal privilege or a confidential record, such as a medical record.

Clause 3(4) provides that where an OPO is sought against a telecommunications provider, communications data is classed as excepted data.[18]

Clause 3(5) provides that, for the purposes of a terrorist investigation (other than a terrorist financing investigation), confidential personal records do not count as excepted data.

3.5 Requirements for making an OPO

Clause 4 sets out the requirements that must be fulfilled in order for a judge to grant an OPO. The judge must be satisfied that there are reasonable grounds for believing the following:

[18] Communications data is defined in the Bill by reference to the Investigatory Powers Act 2016. It is described in the explanatory notes as "data which relates to the communications rather than content".

- That that the person against whom the order is sought operates, or is based in, a country or territory which is party to a designated international cooperation arrangement;
- That an indictable offence has been committed and legal proceedings have commenced or an investigation is under way. This requirement does not apply in the case of a terrorist investigation;[19]
- That the person against whom the order is sought has some or all of the data in question;
- That the data is likely to be of substantial value to the legal proceedings or investigation;
- That it is in the public interest for the data to be made available.

Clause 4(1) provides that the Secretary of State may make regulations to create additional requirements.

3.6 Content, effect, variation or revocation of an OPO

Clauses 5-8 make provision for the content and effect of an order; for the procedure for varying or revoking an order; and for the inclusion of a non-disclosure requirement.

Clause 5 sets out what a judge would need to specify in the order, in terms of the electronic data covered, the person to whom it should be given and a deadline for production. If parts of the application did not meet the clause 4 requirements, the order could specify only some of the data sought.

Clause 8 would allow the judge to include a non-disclosure requirement. This would mean that the person against whom the order was made could not disclose its existence or contents without leave of the judge or written permission from the appropriate officer.

Clause 6 defines the form in which the data should be produced, namely, in a form in which it could be taken away, and in which it was, or could readily be made, visible and legible. It also provides that a requirement to produce or give access to electronic data would apply regardless of where the data was stored, and that it would have effect notwithstanding any other restrictions on the disclosure of information.

Clause 7 would enable a judge to vary or revoke an 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)

[19] According to the explanatory notes, this reflect the position with respect to domestic production orders, para 31

- The Lord Advocate or a procurator fiscal (in respect of Scotland)

An application to vary an order could be made to seek data not covered by the original order, although this could only be granted if requirements of section 4 were met.

3.7 Contempt of court

Clause 11 provides that rules of court may be used to specify the process that should be followed by the court with respect to OPOs. The explanatory notes point out that non-compliance with an OPO could give rise to Contempt of Court proceedings.

3.8 Confidential journalistic data

Clause 12 provides that if there are reasonable grounds for believing that the electronic data sought included 'confidential journalistic data' then the application for the order must be made 'on notice'. This would enable those on notice, such as a journalist whose confidential data was sought by an order, to be a party to the application.

Confidential journalistic data is defined as data which:

- Was created or acquired for the purposes of journalism;
- Is stored by or on behalf of a person who created or acquired it 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

According to the explanatory notes, it will be for the judge to decide who should be put on notice.[20]

Clause 13 provides that a person who has been put on notice under clause 12 (or otherwise) must not conceal, destroy , alter or dispose of any of the data being sought, or disclose the application, without the leave of the judge or the written permission of the appropriate officer.

[20] Para 55

BRIEFING PAPER
Number 8449
30 November 2018

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcenquiries@parliament.uk.

Disclaimer