The Crime (Overseas Production Order) Bill ('The Bill')

The UK authorities are soon to have their powers of investigation extended significantly by a piece of legislation currently going through Parliament. Powers that will mean access to data stored overseas in the name of criminal prosecutions. More worryingly, access to material without being scrutinised by a UK Judge. Having completed its third reading in the House of Commons and about to return to the House of Lords for further consideration, this bill is speedily and silently making its way towards becoming law. **Yasin Patel** and **Amy Hazelwood** consider the bill, its contents and the dangers to individual rights and protections unless the bill introduces and provides more safeguards and protections.

The Bill

In legal jargon, it is a court order that permits law enforcement agencies to require a person or organisation in a foreign jurisdiction to grant access to or produce electronic data that they hold. In essence, the Bill seeks to make it easier for UK authorities to access data stored overseas by foreign technology companies: be they telephone companies, internet providers, social media sites and any other provider with whom you may have an account or used. As stated above, the Bill is now being further considered by the House of Lords having gone back and forth between the Commons and the Lords.

USA

Interestingly, and not so long ago to The Bill's being debated in the UK, on the 23rd March 2018, the USA passed the Clarifying, Lawful Overseas Use of Data Act (the CLOUD Act). The CLOUD Act allows federal law enforcement to compel U.S based companies, via a warrant or subpoena to provide requested data stored on servers, regardless of whether the data is stored in the USA or overseas.

Reciprocity

Crucially for the UK, the CLOUD Act enables foreign governments to enter into new bilateral agreements with the USA. Once a bilateral agreement is entered into, it allows the contracting countries to make data enforcement requests directly to American companies. They will therefore no longer need to go through the US Government under the Mutual Legal Assistance Treaty (MLAT). These are agreements between two or more countries that allow the agreeing

parties to gather and exchange information in order to assist in criminal investigations or proceedings.

The Bill is widely regarded as the UK's reciprocal arrangement to the CLOUD.

The Proposed Law

It is proposed that an applicant for an overseas production order will apply to have produced data that is being stored by a provider abroad. This will be done by an 'appropriate officer': anyone from a constable and financial investigator to a person specified by the Secretary of State. A rather wide and ambiguous list one may think. If the order is made then the person against whom the order is made is required to either:

(a) Produce the electronic data specified or described in the order; or
(b) Give access to the electronic data specified or described in the order.

Personal Records

The data defined by the Bill as "excepted electronic data" cannot be the subject of an Order. "Excepted electronic data" for the purposes of the Bill includes confidential personal records and items subject to legal privilege. "Personal records" include records concerning a person's physical and/or mental health. It also includes records concerning any counselling or assistance pertaining to the welfare of an individual.

The Bill goes on to define what is meant by this. A personal record is confidential if:

1. It was created in circumstances that give rise to an obligation of confidence, and that obligation continues to be owed, or
2. It is held, subject to a restriction on disclosure or an obligation of secrecy contained in law.

A controversial part comes when the Bill goes on to discuss terrorism. The Bill specifies that if an Order is for the purpose of a "terrorist investigation" (other than a terrorist financing investigation), an appropriate officer *may* request access to data that is treated as "excepted electronic data".

"Terrorist investigation" is defined in The Terrorism Act 2000, section 32 as the investigation of:

(a) the commission, preparation or instigation of acts of terrorism,
(b) an act which appears to have been done for the purposes of terrorism,
(c) the resources of a proscribed organisation, and
(d) the commission, preparation or instigation of an offence under this Act

The terrorism exemption is open to abuse given the wide definition of terrorism. This very wide definition, when read together with the Bill, represents a significant increase in law enforcement powers. The Supreme Court stated in their judgement in the case of *R v Gul* [2013] that any legislative narrowing of the definition of "terrorism" is to be welcomed[1].

Whilst such a definition gives law enforcement agencies the power to combat violence perpetrated by terrorists, caution needs to be excised within the context of an Order. Someone subject to an overseas production order under the terrorism exception could find their privacy breached. Accordingly, an overseas production order under the terrorism exception must only ever be used when necessary and with great care. So who is going to ensure that this test has been adhered to?

Death Sentence

The Bill puts in a mechanism in an attempt to ensure that that overseas production orders are not used in proceedings leading to someone being sentenced to death. To this end, the Bill explicitly states an overseas request may not be made of a country or territory in which, a person who is found guilty of a criminal offence, may be sentenced to death under the law of the country or territory in question.

Despite, what on the face of it, appears to be a strong reassurance, the Bill seemingly weakens this safeguard in the proceeding section. The Bill states that the above safeguard does not apply, if the country or territory in question gives assurances that the death penalty will not be imposed in any case in which electronic data is obtained under the Act.

[1] R v Gul [2013] UKSC 64, [2013] 3 WLR 1207; Report, 4.9 – 4.10.

The cause for concern stems from the word, “assurances”.

The UK seeking assurances that the death penalty will not be used in investigations the UK are party to is a long-standing principle. However, this principle recently came under scrutiny in the case of Alexanda Kotey and El Shafee Elsheikh. The allegation they are facing is that they were members of an execution cell in Iraq and Syria who are responsible for murdering captives in these counties. They are currently being held by authorities in America. Under an MLA agreement between the UK and USA, the UK agreed to provide intelligence to assist American authorities in their investigation. However, as the UK agreed to co-operate, the UK did not seek assurances that the death penalty will not be used.

Official Home Office guidelines state 2 very clear principles:

1. If the death sentence is a possible sentence or penalty for the offence under investigation, an assurance that such a sentence will not be carried out or will be commuted.

2. If the execution of the request risks the imposition of the death penalty, this may amount to a ground for refusal[2].

Whilst this oversight happened under what will be the old regime of MLA’s, the warnings are analogous. The Government’s failure to seek assurance that the death penalty would not be used, highlights a central pitfall in the UK legislation. In no part of the Bill is the following specified:

a) Exactly what assurances will be required?
b) From whom such assurances should be sought
c) How those assurances will be obtained
d) The consequences that shall follow, should the assurances not be maintained
e) Who is responsible for obtaining and enforcing the assurances

[2]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415038/MLA_Guidelines_2015.pdf

The Bill provides the perfect opportunity to not only clarify what is meant by the term "assurances", but to codify in law a set of requirements that must be met before, during and after such assurances are sought. However as yet, this is no-where to be seen.

Test for Making an Overseas Production Order

In order to make an overseas production order, the Judge must be satisfied that that there are reasonable grounds for believing that the person against whom the order is sought operates or is based in a country outside of the UK which is party to or participates in the designated international co-operation agreement. The 'designated international co-operation agreement' was discussed earlier in specific reference to the CLOUD Act.

Once a person subject to a COPO has been identified as an individual who operates or is based in a country outside of the UK, the person in question must then be someone who either:

a) Creates;
b) Possesses;
c) Communicates; or
d) Stores the data by electronic means in that country.

The Bill specifies that this applies to individuals, body corporates in the territory and places of business.

The Bill is clearly trying to avoid tactics used by companies to avoid data legislative measures. For example, a corporate body or individual may have their offices in country X and create, possess, communicate with or store their servers and data in country Y that is not subject to data legislation. This part of the Bill is a detailed and deliberate attempt to ensure an overseas production order can be used regardless of such practises.

The Judge must then be satisfied that there are reasonable grounds that an indictable offence has been committed. Proceedings for the offence in question must have instituted or be in the process of being investigated.

With regards to terrorism, the judge must be satisfied that the order is sought for the purposes of a terrorist investigation. As discussed above, 'terrorist investigation' is given a wide

definition. The Bill's omission of the 'reasonable grounds' test when it is a terrorist investigation is cause for concern. By not requiring reasonable grounds the section eradicates any sort of threshold that could have been in place and throws the law back to Terrorism Act 2000 definition.

The Judge must be satisfied that,

a) the person subject to the overseas production order has possession or control of all or part of the electronic data, and
b) that all or part of the electronic data sought by the overseas production order is likely to be of substantial value to the proceedings or investigation that is underway.

The Judge must then enter a balancing act between the public interest on the one hand, and the interests of privacy on the other. In this exercise, the Judge is to have regards to:

(a) The benefit accrued to the proceedings or investigation if the data is obtained; and
(b) The circumstances under which the persons the overseas production order is sought, has possession or control of any of the data.

This is vague, and there is no clarification within the Bill of the threshold that the appropriate officer is required to meet.

Non-Disclosure Requirement

In making an overseas production order, the Judge may impose a non-disclosure requirement on the person who is subject to the order. The non-disclosure order will prevent the person who is subject to the order from:

(a) Disclosing that the order is made; or
(b) Disclosing the contents of the order made, unless they have permission from the judge or an appropriate officer

This has significant consequences for open justice as it will not be in the public domain that a company or individual is subject to an overseas production order.

Overarching Concerns

The Bill gives authorities the power in this country, to access data in other countries. The CLOUD Act does the same with regards to America. Over time, it seems likely that more and more countries will legislate for reciprocal arrangements with other countries. One concern regarding the Bill follows from this almost chain reaction initiated by the CLOUD Act and the Bill subsequently. When a foreign country applies to make an overseas production order for a British national or company based here to produce stored electronic data or give access to it, how does the UK ensure that the other country incorporates the same standards and criteria, and interpretation of those criteria, that would apply to UK courts, before making an order in that other country?

Put another way, how will the UK satisfy itself that the other country making such an order are interpreting the requirements with regards to making an overseas production order, in the same way that the UK anticipates that its courts will be interpreting the law in deciding whether an order should be granted or not.

It is a concern that this Bill does not in any way outline guidelines, or minimum standards that could be in place as requirements for countries applying from overseas to access data in the UK. To this end, the Bill does not specify what can be done if concerns arise that the overseas country have not been implementing a satisfactory interpretation of the criteria for determining whether to make an overseas production order. Accordingly, efforts must be made to specify the following:

a) The means available to stop the order from being enforced against the company or person in the UK if there are concerns.
b) Specify a person, body or authority in the UK who can nullify the production order in question.
c) The basis for making or declining an overseas production order.

These measures need to be in place before the Bill becomes an Act of Parliament, particularly as the Bill will allow greater speed in comparison to the MLA. One possible solution is to include in the Bill a right of appeal in this country against an overseas production order that is applicable here but has been made in another country with which the UK has a bilateral co-operation agreement.

The presumption appears to be that there will be no change, in either direction under the new overseas production orders, in comparison to the MLA arrangements. The problem with this approach is that under the new orders, there has to be a change. This is because, under the current system, it is the court in the country in which the order for electronic data has to be executed that makes the order. Under the new arrangements in the Bill it will be the court in the country where the order is being sought, and not executed, that will make the order and determine whether or not the case for the overseas production order has been established.

Speed is one of the key principles behind the Bill. It is the intention that the Bill will be far quicker by enabling UK courts to issue a production order rather than requesting a foreign court to do so following an MLA request. To this end, the Bill does not specify a timescale within which it will be expected that an overseas production order will produce the requested data or give access to it.

It is anticipated that there will be compliance with an overseas production order that has been made in a UK court. However, the Bill does not set out what will happen in the event that if an individual or company declines to comply with the order. To this end, the CLOUD Act, and the Bill may be all bark and no bite. Both pieces of legislation or any agreement made under it do not create a legal obligation for US individuals or companies to comply with a data request from an overseas Government.

Non-compliance with the Bill may lead to contempt of court proceedings. If this is to be the preferred route to address non-compliance it is is missing from the Bill. A further aspect that needs to be addressed within the Bill is what is to happen if the company or person in this country named in an overseas production order from another country refuses to give access to the data sought under the order.

Whilst the objectives within the Bill are commendable, the concerns raised in this article suggest there is a lot of work to be done before it becomes an Act of Parliament.