Cooley

The US-UK Data Access Agreement: A new dawn for transatlantic criminal investigations?

May 1, 2020

In June 2019 we wrote about the Crime (Overseas Production Orders) Act 2019 (COPOA), an unheralded piece of legislation that created a framework for the government to enter reciprocal agreements with other nations to streamline the process of obtaining stored electronic data from companies based overseas.

In October 2019, the UK home secretary and US attorney general signed one such reciprocal agreement, the US-UK Bilateral Data Access Agreement (the Agreement), which is due to take effect this year. Announcing the Agreement, Home Secretary Priti Patel stated: “This historic agreement will dramatically speed up investigations, allowing our law enforcement agencies to protect the public.” The announcement explains that “under the current MLA process, requests for data can often take anywhere from 6 months to 2 years. Once in place, the agreement will see the process reduced to a matter of weeks or even days.”

Once the Agreement takes effect, US communications service providers should expect to begin receiving overseas production orders (OPOs) directly from the UK on behalf of UK enforcement agencies, including the Serious Fraud Office, National Crime Agency, Financial Conduct Authority and police, to obtain evidence. Likewise, UK-based providers should expect to begin receiving orders directly from US authorities.

Recipients of an OPO issued by the UK will have, as a default, seven days to produce the data stipulated to the UK authorities. Failure to comply with the order may render the recipient in contempt of court. A person cannot be extradited for such a contempt, so in theory it could be difficult for the UK to force compliance with an OPO. However, in reality, being found in contempt of court and the associated publicity and reputational damage is likely to be an unattractive prospect for most companies. An additional important consideration to bear in mind is that a director or officer of the recipient company can in certain circumstances be held personally liable for a contempt of court and could be arrested if they were located within or traveled to the UK. The penalties for contempt of court are imprisonment or an unlimited fine.

Although the aim of OPOs is to significantly speed up the process for UK law enforcement to gather evidence, it also represents a radical change in process, which we expect will generate a raft of legal challenges to OPOs in order to protect the recipient’s interests and rights and produce a number of practical challenges for companies.

The old system

Previously, if UK enforcement agencies wanted to obtain data from a US communications service provider, in the main they were reliant on the mutual legal assistance process (MLA). MLA involves the UK authorities formally requesting assistance from an executing authority in the country to which the request is made. Where the provision of evidence requires a coercive measure, it is sanctioned by the judicial authorities in the overseas jurisdiction. MLA requests from the US to the US for data held in the US are therefore subject to the scrutiny of the US courts and can be challenged in the US, subject to US law and procedure.

The new system

The COPOA allows UK authorities to bypass the MLA process and apply to the UK courts directly to compel a US communications service provider to provide data under an OPO.

The COPOA is a significant departure from the MLA process in that US companies wishing to challenge an OPO will now be forced to do so principally in the UK, under English law and procedure, rather than in the US.

The COPOA provides for an “appropriate officer” from an enforcement agency to make an application to the Crown Court for an OPO. A judge may make an OPO against a US communications service provider where there are reasonable grounds for believing:

- that the recipient is based in or operates in a country or territory outside the UK which is a party to an arrangement such as the Agreement;

- that there is an ongoing investigation or proceedings in respect of any indictable offence;
- the recipient has possession or control of all or part of the electronic data specified;
- that all or part of the electronic data is likely to be of substantial value to the proceedings or investigation;
- that all or part of the electronic data is likely to be relevant evidence in respect of the offence; and
- that it is in the public interest for all or part of the electronic data to be produced or accessed, having regard to
    - the benefit likely to accrue, if the data is obtained, to the proceedings or investigation; and
    - the circumstances under which the recipient has possession or control of any of the data.

Once an OPO is issued by the court, it will be served directly on the recipient by the UK secretary of state. Importantly, the OPO does not require the production of "excepted material," which includes items subject to legal privilege and confidential personal records.

Neither the COPOA nor the Agreement prohibit companies from encrypting data and impose no obligation to de-encrypt data.

Challenging an OPO

The new legislation is widely anticipated to be a game changer in terms of the substantial volume of data that will most likely be obtained on both sides of the Atlantic and the anticipated speed of response by recipients of the OPOs. However, there are a number of important areas that may merit challenge at least in the short term, whilst a workable process is established.

Recipients of OPOs will want to ensure they are in a position to comply lawfully with OPOs, whilst avoiding handing over data in circumstances where they may breach other legal duties to their customers and the attendant risk of potential follow-on litigation.

One of the first actions taken on receiving notice of an OPO application may well be to request further time to comply. It is anticipated that such requests will be granted so that many of the novel issues and challenges arising from the COPOA and Agreement can be given due consideration.

US recipients of an English OPO will be able to apply to vary or discharge an OPO in the English crown courts and may be able to challenge them by way of judicial review in the High Court. As with other domestic search warrants and production orders, a vast number of potential challenges could be made to an OPO depending on the facts of each particular case. By way of example, there may be arguments that a request is too broad, that the recipient is not in possession or control of the data, that it is not in the public interest for all or part of the electronic data to be produced or accessed, or that other conditions that must be met in order to grant an OPO are not satisfied.

Data protection issues will need careful consideration, particularly when data is held in a country outside the UK or US. While the COPOA does not require a recipient to do anything that would breach the UK data protection legislation, the data protection law of other jurisdictions, such as France, may prevent the disclosure of the data in the absence of an international treaty like the Agreement being entered into by that country.

Preventing the disclosure of privileged material is also likely to present important legal issues for the recipient, which will give rise to potential challenges. For instance, while the COPOA makes plain items subject to legal privilege fall outside of the proper scope of an OPO – and privilege is defined with reference to English law – it remains to be firmly established whether there is scope for arguing against compliance on the basis that the requested material is privileged under US law. Existing English case law suggests that even where it is accepted that documents are protected by privilege under US law, if the documents are not protected by privilege under English law they will be disclosable in English proceedings. However, further judicial clarity regarding the position may well be sought once OPOs are brought into force either by way of an application to the Crown Court in the first instance or subsequently by judicial review.

Judicial guidance may also need to be sought to clarify the methodology that should be applied to determine the extent of privileged material given that in most instances the recipient of the OPO will not be the privilege holder, and a non-disclosure order may prohibit the recipient from disclosing the existence of the order to anyone.

In addition, each OPO must be reviewed by the secretary of state and can only be served on the recipient if the secretary of state certifies in writing that they consider doing so would be in accordance with the Agreement. Separately to the Crown Court process, the Agreement specifically provides another mechanism for challenge, under which recipients of an OPO who believe the Agreement may not be properly invoked may raise objections in the first instance to the issuing party's designated authority. The Agreement and COPOA contain some separate provisions that mean this mechanism

will have to be invoked where the COPOA has not imported requirements contained within the Agreement. By way of example, an OPO cannot intentionally target certain categories of individuals or entities (such as a citizen or national of the US, to give one example) under the Agreement, but the COPOA does not contain these exclusions.

The UK's designated authority must respond to the objections, and if they are not resolved, the recipient may raise the objections to their own country's designated authority. The two countries' designated authorities may then confer in an effort to resolve the objections.

It seems likely that challenges to the new powers may also be made in the US courts on the basis that OPOs issued in the UK violate fundamental or constitutional rights under US law. You can read more about potential challenges in our recently posted article on the topic.

The future landscape

The US is reportedly in negotiations with the European Commission and Australia to negotiate equivalent data sharing agreements. Other countries likely to follow suit are New Zealand and Canada.

Many OPOs will be served on companies that otherwise have no involvement in an investigation and that would previously have been regarded by enforcement agencies as out of reach on a practical basis.

Any parties served with an OPO are best served to seek legal advice as soon as possible to ensure suitable steps are taken to challenge the order, if necessary, and ultimately to assist in successful compliance with the order and balance the various competing interests whenever possible.

Companies that are likely to receive multiple OPOs would be especially well advised to consider designing a suitable system for handling OPOs and become familiar with the types of issues that may give rise to challenges, some of which are touched on above.

The COPOA and the Cloud Act Agreement seem likely to bring a torrent of litigation and we shall see if the process is in fact speedier as a result of their implementation.

If you have any questions or would like to find out more about this topic, please contact Tom Epps, Sascha Grimm, William Schwartz, Andrew Goldstein, Daniel Grooms, Marie Kavanagh or Oliver McGlashan.

Notes

Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, 3 October 2019

https://www.gov.uk/government/news/uk-and-us-sign-landmark-data-access-agreement

The judge approving the OPO may grant a longer or shorter period as appropriate

The SFO can also, under certain circumstances compel the production of documents held overseas by a company with no presence in the UK under section 2(3) of the Criminal Justice Act 1987, following the decision in R (on the application of KBR Inc) v The Director of the Serious Fraud Office EWHC 2012 (Admin) The SFO's assertion that section 2(3) had extraterritorial effect in that case was challenged on jurisdictional grounds but the High Court held that in the circumstances of that case, there was a 'sufficient connection' between KBR Inc. and the UK KBR Inc. is appealing the decision to the Supreme Court and the decision has been widely criticized by legal commentators

Under Section 4(11) of the COPOA "relevant evidence," in relation to an offence, means anything that would be admissible in evidence in proceedings in respect of the offence

This requirement does not apply where the data in respect of which the OPO is sought, is for the purposes of a terrorist investigation

The RBS Rights Issue Litigation EWHC 3161 (Ch)

Contributors