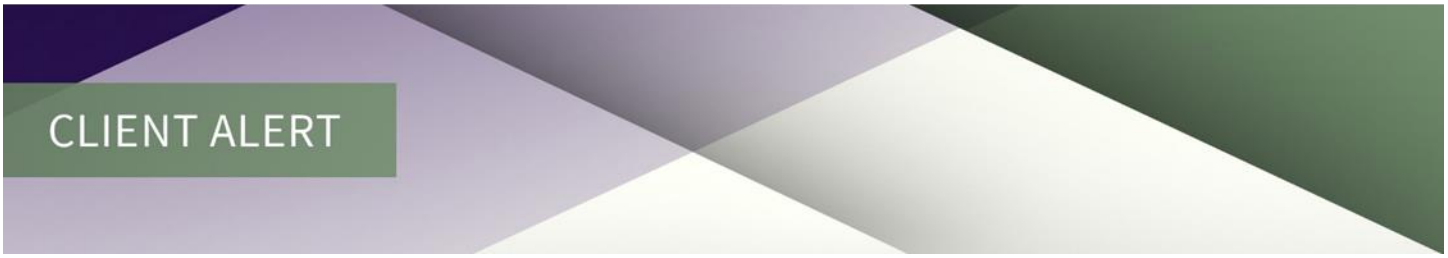

UK Enforcement Authorities Given New Powers to Obtain Electronic Data Stored Overseas

May 3, 2019

AUTHORS

Peter Burrell | Francesca Sherwood

The Crime (Overseas Production Orders) Act 2019 ("**COPOA**"), which came into force in February 2019, significantly extends the powers of UK enforcement authorities, such as the Serious Fraud Office ("**SFO**") and the Financial Conduct Authority ("**FCA**"), to obtain electronic data from overseas service providers.

Background

Pursuant to section 2(3) of the Criminal Justice Act 1987, the SFO has the power to issue a notice requiring a person or entity under investigation, or another person, to produce documents which appear to relate to any matter relevant to an investigation (a "**Section 2 Notice**"). In our briefing in January, we discussed the recent decision in *R (on the application of KBR Inc.) v SFO*[1] in which the High Court determined that a Section 2 Notice could require the production of documents held overseas by a foreign company, provided that the foreign company had a "sufficient connection" to the UK.

Where data is held overseas but there is no "sufficient connection" to the UK, the Mutual Legal Assistance ("**MLA**") regime is often the only way by which enforcement authorities can obtain relevant documentation. However, the MLA regime is a notoriously slow process and, as a result, poses difficulties to enforcement authorities in concluding timely investigations or prosecutions.

[1] *R (on the application of KBR Inc.) v SFO* [2018] EWHC 2368 (Admin).

Bypassing overseas authorities, the procedure under the COPOA is a significantly easier and faster way to obtain data held overseas, as a party served with an Overseas Production Order ("**OPO**") has only seven days to either produce the data or provide access to it. This could be a very costly and time-sensitive exercise for the recipient, depending on the scope of the OPO.

What is an OPO?

The COPOA provides that an "appropriate officer" can make an application for an OPO. An "appropriate officer" includes members of the SFO, FCA and officers of HM Revenue and Customs.

An OPO can be made in respect of "electronic data", which is broadly defined as "any data stored electronically". However, the COPOA specifically excludes data that is either subject to legal professional privilege or is confidential personal data. If the target of an OPO is a telecommunications operator[2], communications data is also excluded.

In making the OPO, the judge needs to be satisfied that there are reasonable grounds for believing that an indictable offence has been committed and that either the offence is being investigated or proceedings have been brought. An OPO is also available for the purposes of a terrorist investigation. The data must be likely to be "relevant evidence" in respect of the offence (save where it relates to terrorism) and of substantial value (whether or not by itself) to the investigation or proceedings. "Relevant evidence" is defined as anything that would be admissible in evidence in proceedings in respect of the offence.

The enforcement authorities must also satisfy a public interest test by demonstrating that production of all or part of the electronic data is in the public interest having regard to the likely benefit it will have in the investigation or proceedings and the circumstances in which the recipient of the order is in possession of that data.

Against Whom Can an OPO be Made?

Whilst the COPOA does provide significantly broader data-gathering powers, the individual or entity against whom an OPO is made must operate in a territory which is party to a designated international cooperation arrangement with the UK.

The UK has not, as yet, concluded any such arrangements, although negotiations with the US are ongoing. The US passed its counterpart to the COPOA last year, in the form of the Clarifying Lawful Overseas Use of Data Act (also known as the CLOUD Act), which gives US enforcement authorities extra-territorial data-gathering powers, subject to there being data-sharing agreements in place with other jurisdictions. No such agreements have been entered into as yet.

[2] As defined in s. 261 of the Investigatory Powers Act 2016.

As a result, until an international cooperation arrangement is finalised, UK enforcement authorities will have to continue to rely on the existing MLA regime.

An individual or entity affected by an OPO can apply to the English courts for revocation or variation of the OPO, to compensate in part for the fact that the relevant authorities in the overseas country will no longer be able to scrutinise a data request as they would under an MLA request.

Non-Disclosure of an OPO

A significant development is that an OPO can include a non-disclosure requirement, preventing the individual or entity from notifying any other party of the OPO, thereby reducing the risk of the recipient tipping off the party under investigation, which may be unaware of the investigation at that stage. The degree to which such a requirement is enforceable against an overseas individual or entity is, however, uncertain.

Conclusions

Whilst the COPOA appears to give enforcement authorities extensive data-gathering powers, it is unlikely that we will see OPOs being granted in the near future. However, once a cooperation agreement is achieved with the US, US companies are likely to face OPOs going forward as a means for UK authorities to swiftly access data held by them, particularly given that major internet and social media companies are based in the US.

Companies or individuals that receive an OPO in due course will also need to consider any conflict between complying with the OPO and complying with local laws, given the increased focus on data protection and the cross-border transmission of data.

Willkie Farr & Gallagher has significant experience in advising companies on multi-jurisdictional investigations and navigating compliance with the Section 2 Notice regime with considerations of cooperation, data protection and other local laws.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Peter Burrell
44 20 3580 4702
pburrell@willkie.com

Francesca Sherwood
44 20 3580 4749
fsherwood@willkie.com