Overseas Production Orders – UK law enforcement agencies have new powers to compel disclosure of electronic data stored abroad (well, not quite yet)

Published 22 May 2019

On 12 February 2019, the Crime (Overseas Production Orders) Act 2019 came into force. Its aim is to assist law enforcement agencies speed up the process of obtaining disclosure of electronic data stored outside of the UK for use in criminal and regulatory investigations and prosecutions in the UK. Whilst the Act is in force, it is not yet capable of being used by law enforcement agencies because it can only operate where there are, in place, "*designated international co-operation arrangements*" which provide for mutual assistance in connection with investigation or prosecution of offences. Such designated co-operation arrangements will, in time, be ratified and designated by the Secretary of State. It is understood the first such designated co-operation agreement is likely to be agreed between the UK and the US.

So, what's the big deal?

Historically, the production of evidence from overseas for use in UK prosecutions has been a long and drawn out (and uncertain) process. The UK law enforcement agencies have had to rely on the provisions of Mutual Legal Assistance ("MLA") treaties which can take months, sometimes years, to bear fruit. For some UK law enforcement agencies, the only means to a quicker process has been through the ability to find some corporate presence in the UK or some unwitting officer or individual capable of being served with process in the UK[1].

Criminal wrongdoing is, more than ever before, gaining international dimensions. Moreover, the physical location of evidence has become a more common and complex issue with the predominant use of electronic communications and the plethora of communication platforms and applications available to the public. Whilst UK law enforcement agencies have effective means of gathering electronic data in the UK, they are currently stuck with slow and cumbersome MLA provisions to obtain evidence that is truly located outside of the jurisdiction.

So what are OPOs?

UK law enforcement agencies (which includes the SFO, NCA, police, HMRC and the FCA) can apply to the Crown Court for an Overseas Production Order ("OPO") to require a person based overseas to produce or give access to electronic data regardless of the location in which it is stored.

In making an OPO, the Judge must be satisfied that there are reasonable grounds for believing that:

- the person against whom the order is sought operates or is based in a country outside the UK which is a party to, or participates in, a designated co-operation arrangement;
- an indictable offence has been committed and proceedings in respect of the offence have been instituted or the offence is being investigated;
- the person against whom the order is sought has possession or control of all or part of the electronic data;
- all or part of the electronic data sought is likely to be of substantial value to the proceedings or investigation;
- all or part of the electronic data sought is likely to be relevant evidence in respect of the indictable offence committed or the offence being investigated;
- it is in the public interest for all or part of the electronic data sought to be produced.

The Act does provide for the protection from disclosure of legally privileged data and confidential personal records.

A person served with an OPO has 7 days in which to produce or give access to the electronic data sought. The person served or any interested party, has the ability to challenge the OPO but only by application to the issuing Court in the UK – they can no longer challenge the disclosure requirement in their own local courts.

So this is a good thing, right?

In true fence sitting style, the answer is both yes and no. For the law enforcement agencies, of course, yes, it will help speed up the process of obtaining important electronic evidence for use in investigations and prosecutions. The electronic data obtained under an OPO is directly admissible in criminal proceedings. The downside for the law enforcement agencies

is that, unfortunately, international fraudsters can be quite sophisticated and will be forever driven to use more creative and devious means through which to orchestrate their schemes.

For the persons anticipated to be the most common recipients of an OPO: social media platform providers, encrypted communication services providers, telecommunications service providers, the answer is most likely yes and no in equal measure. On the one hand, they are subject to clear provisions that takes the substance of the decision out of their hands. However, it does create an extra burden in considering issues such as legal privilege and what constitutes confidential personal records.

For subjects of criminal investigations and prosecutions, of course, it's a bad thing. However, pausing here for a second: not every subject of an investigation or prosecution is a bad person. One wrinkle in the Act is that OPOs can be obtained without notice to the subject. This prevents the subject from being able to make representations to the issuing Court about the compulsion of the electronic data before it is disclosed to the UK law enforcement agency. That in itself is no major change to the regime because evidence obtained under an MLA is more often than not obtained under a necessary veil of secrecy, especially where it occurs at the investigation stage. But, where evidence obtained via an OPO becomes admissible in criminal prosecutions without qualification, that is potentially a big deal for a subject who, it would appear, no longer has an ability to challenge admissibility.

Great, so OPOs look like a pretty cast iron way to compel disclosure of electronic evidence, right?

Yes they do – or rather they will once designated co-operation arrangements are in place. In real terms, the Act creates a tool which the UK law enforcement agencies will be able to use to obviate legal and technical obstacles which have surrounded the compulsion of electronic evidence where the ability to actually locate that data has become ever more complex.

The only potential issue for UK law enforcement agencies is the lack of an effective sanction for non-compliance with an OPO – contempt of court is all that the directors of the person served with an OPO have to fear if they fail to comply. Whilst contempt of court is no laughing matter, it has little impact for a director located in a different jurisdiction who cannot be extradited for it. Of course, there are reputational issues to consider and for companies that operate on a global basis, not co-operating with criminal authorities may bring unwanted criticism or scrutiny.

One final point arises in relation to the nature of electronic evidence – unlike physical evidence, it is not static: it can change when accessed or processed. Presently, the Act requires a person served with an OPO not to "conceal, destroy, alter or dispose" of the electronic data sought. "Alter" may become an issue where accessing or processing data leads to altering it and where the capture of metadata[2] has increasing significance, this is a real issue that will need to be addressed.

Once OPOs become effective, there will undoubtedly be issues and challenges to the regime it creates. Whether they arise from the issues identified above or otherwise waits to be seen.

[1] S.20 PACE 1984, s.2(3) Criminal Justice Act 1987 and in R(on the application of KBR Inc) v Director of the Serious Fraud Office) [2018] EWHC 2368 (Admin), s.7 Crime (International Cooperation) Act 2003.

[2] Metadata is data (information) that provides information about other data. It is often used to provide a reliable audit trail around the life of an electronic document.

Authors

Jonathan Brogden
London - Walbrook
+44 (0)20 7894 6290
jbrogden@dacbeachcroft.com