Overseas Production Orders—the corporate investigations perspective

18/06/2020

Corporate Crime analysis: Rebecca Niblock, partner at Kingsley Napley, examines the US-UK Bilateral Data Access Agreement (the Agreement) expected to come into force in July 2020, and considers some of the questions arising for corporates around Overseas Production Orders (OPOs).

What are the practical implications of the implementation of the Agreement from a corporate crime perspective?

While a focus for the Agreement has been the investigation of terrorism and child abuse, an OPO can be granted for the purpose of the prevention, detection, investigation or prosecution of a serious crime which is one that could result in a custodial sentence with a maximum possible term of at least three years. Serious fraud, bribery and corruption fall within this category and it is likely the Serious Fraud Office (SFO) and other law enforcement authorities will want to use these new powers to bolster their investigations into both individuals and corporates. As Lisa Osofsky, director of the SFO, famously stated early in her tenure, 'I intend to use all the powers at my disposal…My approach will be international, cooperative across all jurisdictions…'

Unless and until the law of corporate criminal liability is reformed, electronic evidence which goes to 'the acts and state of mind' of those who represent 'the directing mind and will' of the company is essential to the SFO. Investigations into failure to prevent bribery or the facilitation of tax evasion will also look to electronic evidence of employees' or agents' actions. As the current circumstances of the pandemic exemplify, when virtually all business must be conducted electronically, a simplified and expedited process which enables law enforcement authorities to obtain electronic data in the months to come may well prove irresistible.

We already have formal evidence and investigation output sharing arrangements (mutual legal assistance arrangements) and various informal arrangements so, from the perspective of the additional advantages/disadvantages of OPOs, how are corporates likely to be impacted by these developments?

Pursuant to the Stored Communications Act in the US, there are a number of constraints on the sharing of electronic data with UK law enforcement authorities. These constraints mean that to date UK law enforcement authorities have been reliant upon the mutual legal assistance (MLA) regime to access the data (rather than relying on informal arrangements). An MLA request to US authorities to access electronic data stored in the US, where most of the communication service providers (CSPs) are based, can take between six months and two years to be processed. It is a cumbersome and time-consuming process which many believe is ill equipped to cater for the ever-increasing reliance upon electronic evidence to prosecute criminal cases. According to a 2018 European Commission impact assessment report, more than half of all criminal investigations include a cross-border request to access electronic evidence.

In contrast, upon receipt of an OPO a CSP will have the default time limit of seven days in which to produce the data requested. In practice a UK judge can and is likely to allow a longer time period for requests for large quantities of data but even then, the whole process will be significantly quicker than under the current regime. This expedited procedure should reduce the risk of an investigation into a corporate and its officers being abandoned or delayed due to a UK law enforcement authority's inability to access the data. It may also allow investigators access to material that they might have previously dismissed as being inaccessible.

Note also that a corporate which is the focus of the underlying investigation is likely to be unaware of the order at the time as the judge can include a nondisclosure requirement with the OPO.

The process for obtaining data pursuant to an OPO is not without difficulty in that the Agreement does not require CSPs to provide data in a legible format or to decrypt data. CSPs are also able to challenge the OPO and its terms in a UK court, and undoubtedly teething difficulties with interpretation and legal challenges will lead to delays when the Agreement does come into force.

References:
R (on the application of KBR Inc) v The Director of the Serious Fraud Office [2018] EWHC 2368 (Admin), [2018] All ER (D) 12 (Sep))

Pending an appeal to the Supreme Court in the case of *R (on the application of KBR Inc) v The Director of the Serious Fraud Office*, the SFO can also compel production of documents held overseas by a company with no presence in the UK (under section 2(3) of the Criminal Justice Act 1987) and so could obtain electronic data in this way. However, there would have to be 'a sufficient connection' between the UK and the company being compelled to produce the evidence, and the notice must be served within the UK. So arguably an OPO is a more straightforward route as it does not require such a nexus.

How would a corporate facing a multi-jurisdictional, multi-agency investigation be the subject of these data sharing powers? How, realistically, would that impact the corporate?

The impact of these data sharing powers may not be as great on corporates facing multi-jurisdictional, multi-agency investigations because different agencies may be able to collaborate and share information between them without the need for an OPO (although there can be admissibility issues to overcome for evidence received in this way). There is, for example, already a strong record of co-operation between the SFO and its US counterparts: the recent DPA with Airbus demonstrates the ability of authorities from different jurisdictions to successfully work in parallel.

What do corporates need to consider when conducting internal investigations or considering making a self-report with reference to these new powers?

The advent of OPOs means corporates must consider which CSPs hold their data and where they are located. Corporates should be proactive in this regard and not wait for an event to trigger an internal investigation or the possibility of a self-report. Any internal investigation should include an analysis of the extent to which electronic communications may be stored under personal email, messaging or video conferencing accounts which the corporate may not be able to access but could be obtained by a law enforcement authority using an OPO.

The new powers are unlikely to impact on the benefits to a corporate of making a self-report to the SFO because the SFO will not want to discourage co-operation. Indeed, a corporate may feel incentivised to co-operate by the risk of an OPO in the event that it does not. There may even be benefits to a corporate of the enforcement authority applying for an OPO rather than the company voluntarily disclosing the electronic data it has in its possession in terms of costs, avoidance of any data protection and confidentiality issues, and preservation of digital integrity. The flip side to this are concerns over how legal professional privilege (LPP) will be protected when the CSP in the US will be the person responsible for deciding what, if any, material is privileged.

What impact do you think this might have on the nature of global corporate criminal investigations generally?

The Agreement is the first of its kind under the Crime (Overseas Production Orders) Act 2019 and is likely to be a precursor for agreements with other countries as it is a shining example of the determined push globally for cross-border co-operation and information sharing (the US is already in formal negotiations with Australia for a bilateral agreement). It will be particularly important for the UK who will lose the substantial benefit of information sharing measures between EU Member States when the transition period ends later this year 2020. The ease with which data may be shared across jurisdictions in the future will undoubtedly assist investigators and could mean less reliance upon corporates for disclosure. However, a tool which further increases the quantity of electronic evidence presents its own challenges, and law enforcement authorities will have to work hard to keep pace. The SFO has already faced criticism for the delays in progressing cases and processing electronic data.

Interviewed by Alex Heshmaty.