GIR
Global Investigations Review

What recent US and UK reforms to information sharing mean for cross-border investigations

Ryan Junck, Steve Kwok, William Ridgeway and Elizabeth Robertson
18 July

Ryan Junck, Steve Kwok, William Ridgway and Elizabeth Robertson (Credit: Skadden Arps Slate Meagher & Flom)

Skadden partners Ryan Junck, Steve Kwok, William Ridgeway and Elizabeth Robertson argue that recent reforms in the US and UK make where companies store data increasingly important.

The US and UK governments recently enacted legislation to facilitate access to electronic data stored by technology companies overseas for criminal investigations and prosecutions. These laws enable law enforcement authorities to bypass the often cumbersome and inefficient process of obtaining such data through foreign judicial assistance requests. In the US, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) allows federal law enforcement to compel service providers subject to US jurisdiction to disclose requested data, even when that data is located outside of the US. Service providers transport information electronically, including providers of wireless, landline, cable, satellite, internet and cloud-based communications.

Across the Atlantic, the UK's Crime (Overseas Production Orders) Act (the COPO Act) reflects many of the same principles and potentially goes further by empowering enforcement agencies to compel disclosure from any individual or company operating or based abroad, provided that the UK has a designated international cooperation agreement (DICA) with the country where the production order will be served. The CLOUD and COPO Acts are the first of their kind and reinforce the recent trend of increased cooperation in cross-border investigations, particularly between the US and the UK. More countries are poised to enact similar legislation in an attempt to bypass the existing mutual legal assistance treaty (MLAT) process. However, such legislation could also create obligations conflicting with other jurisdictions' laws, such as those pertaining to bank secrecy and data localisation. In light of this new regulatory landscape, global companies should re-examine their data storage procedures with an eye to addressing future data requests.

First published on the *Global Investigations Review* website, 18 July 2019

CLOUD Act

Congress passed the CLOUD Act in March 2018, catalysed by Microsoft's high-profile litigation against the US government over compliance with a search warrant seeking emails stored by the company in Ireland. The CLOUD Act has two distinct components. First, it allows the US government to enter into deals with other countries that will require communications-service providers subject to US jurisdiction to respond to those countries' requests for data. Second, the Act amends the Stored Communications Act to clarify that companies such as Microsoft and other service providers – including providers of internet service, email, and cloud storage – subject to US jurisdiction must disclose electronically stored data within their "possession, custody, or control" irrespective of the data's location. Companies served with a subpoena or warrant under the law can challenge it on the basis that the user whose data is sought is not a US person or does not reside in the US, or that disclosure would materially risk violating the laws of a foreign government.

The US nexus requirement is broad and could include a service provider accessing the US banking system, using email with a server situated in the US or having business or operations in the US. For example, an overseas service provider with websites that appear to serve US customers may find itself subject to legal process in the US. In response to criticisms about the potential expansion of US jurisdiction overseas, the Department of Justice published a white paper on the CLOUD Act in April 2019 that describes the reasons for the Act's enactment and attempts to dispel misconceptions. The white paper claims that the CLOUD Act did not add new elements to the scope of data ownership but clarified existing requirements on the production of data within a provider's possession or control. Companies are deemed to be in control if they have a legal right or practical ability to access the overseas data, which often cannot be determined without engaging in a fact-intensive investigation of where a company's data resides and how it may be accessed.

COPO Act

While the COPO Act mirrors several aspects of its US counterpart, it goes one step further by providing for the issuance of overseas production orders (OPOs). OPOs require the production of electronic data directly from any legal person (an entity or individual) where a UK court is satisfied that there are reasonable grounds to believe that: (1) the person against whom the OPO is sought operates or is based in a country outside the UK, and which is party to a DICA; (2) an indictable offence has been committed under the applicable UK laws and proceedings have commenced or the offence is being investigated by UK authorities; (3) the person against whom the OPO is sought has possession or control of all or part of the data; (4) all or part of the data is likely to be of substantial value to the proceedings or investigation; and (5) it is in the public's interest for all or part of the data to be produced. Similar to the CLOUD Act, exceptions exist for information covered by legal privilege and confidential personal data. Perhaps the most significant aspect of the COPO Act is that a recipient of an OPO is served directly, and will have a default period of seven days in which to produce the required data. The OPO procedure also removes the supervisory role of any receiving country's authorities which, coupled with the seven-day default period, is intended to guarantee that UK law enforcement receives the data far more quickly than if it relied on the MLAT process. As the COPO Act does not grant UK courts any punitive power, failure to comply with an OPO may at worst result in a contempt of court.

First published on the *Global Investigations Review* website, 18 July 2019

Enhanced cross-border cooperation

Both the CLOUD and COPO Acts provide for pre-qualification agreements – executive agreements and DICAs, respectively – which create a treaty-like information-sharing protocol. Under the CLOUD Act, the US can establish an agreement with another country if it is designated as a qualified foreign government, which will grant reciprocal access to data for the investigation and prosecution of certain crimes. Although no government has yet qualified, the UK is likely to be the first to enter into an agreement with the US, and the European Commission has stated its intention to do so. Once approved, a qualified foreign government will be allowed to serve requests for data directly on the company, rather than on the US government through the MLAT process.

The COPO Act empowers a UK court – at the request of an appropriate officer, as defined in the Act – to require the production of electronic data directly from a person or company overseas through an OPO if the UK has a cooperation agreement with the relevant country. As in the case of the CLOUD Act, no such agreements are yet in place, although a US–UK agreement will likely be the first, as negotiations have been ongoing since 2015. Since the US has the largest number of service providers, British legislators identified the US as one of the countries likely to be most affected by the COPO Act.

Conflicts with other jurisdictions' laws

While the CLOUD and COPO Acts, and similar legislation, may streamline the data-collecting and sharing process, they can create conflicts with other jurisdictions' laws, including bank secrecy and data localisation laws.

Bank secrecy jurisprudence may be informative in predicting how a US court would resolve conflicts involving the CLOUD Act and the laws of another jurisdiction. For example, in the Bank of Nova Scotia subpoenas, which concerned data production requests for overseas bank records, the courts considered whether the domestic bank had a legal right or practical ability to access the overseas records. Even if such access is determined to exist, a court would conduct a comity analysis if compliance with a subpoena could put a company at odds with the laws of the country where the records are stored.

Data localisation laws require that data collected in that jurisdiction remain within it. Such laws have recently been enacted in China, Russia and India. For example, China's recently enacted Cybersecurity Law requires data generated in the regular course of business in mainland China to be maintained there and imposes various restrictions on data transfer and export. This law and similar laws in other jurisdictions may make the CLOUD and COPO Acts increasingly necessary to US and UK regulators, as service providers that used to store data back at company headquarters in the US or in the UK are now required by local law to store locally generated data locally. At the same time, some of these jurisdictions also have blocking statutes to counteract the extraterrestrial application of foreign laws. For example, China's recently enacted Criminal Judicial Assistance Law requires that any information intended to be produced to foreign law enforcement authorities first be provided to the Chinese authorities for review. Together, these data localisation and blocking statutes, by interposing obstacles to the production of information that the CLOUD and COPO Acts make mandatory, may place companies between a rock and a hard place.

First published on the *Global Investigations Review* website, 18 July 2019

Takeaways

Although the CLOUD and COPO Acts signal potential enhanced cross-border cooperation and potential simplification, MLA remains the standard protocol for data transfer because the pre-qualification agreements are not yet in place and also the two acts apply to crimes only. While companies should review their legal process protocols in light of both acts, their impact remains uncertain and the COPO Act's effect on large-scale investigations is probably limited.

In the US, the CLOUD Act confirms that data stored abroad may be subject to compelled production. And in the UK, the Serious Fraud Office and Financial Conduct Authority may soon be able to seek a court order for the production of electronic data held by anyone abroad if the UK has a DICA with the country where the order will be served. Therefore, companies, including both US-based service providers and out-of-country and foreign service providers subject to US jurisdiction, should take planning steps, which may include: (1) mapping their corporate entity details and subleasing agreements so they know who controls what data; (2) reviewing their contracts with service providers, including provisions addressing whether a data centre will be located in a country that has entered into an agreement with the US or a DICA with the UK (once such agreements are reached); and (3) considering the use of client-side encryption for exclusive control by the client. If a data centre is located in a country with an executive agreement, this will better insulate the company from the risk of conflicting obligations under different jurisdictional laws if faced with data requests from US or foreign law enforcement authorities.

With respect to the COPO Act, significant changes to the conduct of cross-border investigations in the near future are unlikely. While OPOs could offer a quicker and less costly procedure than MLA, it seems unlikely that they will be used for large-scale disclosure due to the seven-day production requirement, which is highly compressed for the scale of typical cross-border investigations. Accordingly, the importance of OPOs may be overstated. Moreover, as discussed above, the UK’s enforcement of OPOs is likely to rely on the threat of being held in contempt of court. The amount of influence that this will have over US-based service providers, is questionable.

It remains to be seen if laws like the CLOUD and COPO Acts will significantly change the exchange of electronically stored data between the US and foreign authorities in cross-border investigations. For now, global companies should be keenly attuned to who controls their data and how and where it is stored. They should also pay close attention to the potential enactment of pre-qualification agreements and any changes to laws in other jurisdictions that may affect their obligations to respond to certain data requests.

Not necessarily the views of Skadden Arps or any one or more of its clients.

First published on the *Global Investigations Review* website, 18 July 2019