

CLIENT ALERT

# Landmark Cross-Border Data Access Agreement signed by UK and US

October 31, 2019

## AUTHORS

[Peter Burrell](#) | [Daniel K. Alvarez](#) | [Francesca Sherwood](#)

The UK and the US have entered into a landmark Data Access Agreement that will allow their respective enforcement agencies to request electronic data relating to serious crime directly from tech companies based in the other country.

In our May [client alert](#) we discussed the new Crime (Overseas Production Orders) Act 2019 (“**COPOA**”), which received Royal Assent earlier this year and in principle significantly extended the powers of UK enforcement authorities to obtain electronic data by way of an Overseas Production Order (“**OPO**”) from overseas providers. Whilst negotiations with the US were ongoing at that time, the UK had not entered into any data-sharing agreements with other jurisdictions to enable OPOs to be made. The UK-US Data Access Agreement therefore gives effect to the COPOA.

UK enforcement agencies such as the Serious Fraud Office will now have the ability to apply for an OPO to obtain data directly from service providers based in the US. This Agreement is therefore a landmark development in response to the difficulties faced by enforcement authorities under the existing Mutual Legal Assistance regime in obtaining overseas electronic data, which could take months or even years. This new Data Access Agreement will see the process reduced to a matter of weeks or even days. It will therefore provide enforcement authorities with more efficient and effective access to data, allowing them to conduct more timely investigations or prosecutions.

In the US, the Data Access Agreement is the first bilateral agreement that the US has entered into under the Clarifying Overseas Use of Data Act of 2018 (commonly known as the “**CLOUD Act**”). The CLOUD Act amended the Stored Communications Act in an effort to clarify potential obligations for companies in the US that operated or otherwise stored data outside the US. The CLOUD Act does not change the fundamental requirement that the sought-after data must be in

---

## Landmark Cross-Border Data Access Agreement signed by UK and US

the “possession, custody, or control” of the party from whom the data is being sought, but it does establish mechanisms by which the US government can enter into these kinds of bilateral agreements to facilitate data sharing.

Any request for data must be made under an authorisation in accordance with the legislation of the country making the request and will be subject to independent oversight or review. In the case of an OPO, as set out in our earlier [client alert](#), this will include satisfying a judge that there are reasonable grounds for believing that an indictable offence has been committed, and that the data would be admissible in evidence and of substantial value to the investigation or proceedings.

This may have a significant impact on companies under investigation, as enforcement agencies in the UK or the US would now be able to gather evidence much more quickly, even if it is held in the other jurisdiction. Whilst the terms of the Agreement have not yet been made public, it is expected to enter into force in early 2020, following a review by Parliament and the US Congress.

It has also been made clear that the Agreement does not change anything about the way companies can use encryption, and does not prevent companies from encrypting data. As a result, an open letter addressed to Facebook was published by the UK, US and Australian governments following the signing of the Agreement, outlining serious concerns with Facebook’s plans to implement end-to-end encryption across its messaging service. The letter requested that Facebook halt those plans unless it can provide assurances that they would not compromise user safety and enable law enforcement access to content in exceptional circumstances to protect the public. The view of the UK government is that this exceptional access to data would not undermine its commitment to the right to privacy. Law enforcement must be able to access data, with independent authorisation and oversight, in certain circumstances. It will be important to keep a watching brief on how Facebook and other such companies respond.

---

## Landmark Cross-Border Data Access Agreement signed by UK and US

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](mailto:pburrell@willkie.com)

**Daniel K. Alvarez**

202 303 1125

[dalvarez@willkie.com](mailto:dalvarez@willkie.com)

**Francesca Sherwood**

+44 20 3580 4749

[fsherwood@willkie.com](mailto:fsherwood@willkie.com)

Copyright © 2019 Willkie Farr & Gallagher LLP.

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Palo Alto, San Francisco, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at [www.willkie.com](http://www.willkie.com).