U.K. and U.S. Sign Landmark Cross-Border Data Sharing Agreement

9 October 2019

On 3 October 2019, the United Kingdom and the United States signed a landmark data sharing agreement to give law enforcement agencies in one country faster access to digital evidence held by service providers, such as web hosts and social media companies, located in the other (the "Agreement").[1] With requests under current Mutual Legal Assistance Treaties ("MLATs") taking months or even years, the Agreement aims to reduce wait times to weeks or sometimes days. It is expected to enter into force in the coming months, following review by the U.K. Parliament and the U.S. Congress.

Background. In response to what both governments view as unacceptable delays in obtaining digital evidence overseas under existing MLAT procedures, the U.S. introduced the CLOUD Act in March 2018, and the U.K. introduced Crime (Overseas Production Orders) Act 2019 in February 2019. Under the CLOUD Act, instead of sending an MLAT request through central government, U.S. authorities can request digital evidence directly from an overseas service provider if the U.S. has an executive agreement with that service provider's home country. Similarly, the U.K. Act allows designated authorities—including the Police, Serious Fraud Office and the Financial Conduct Authority—to apply to the U.K. Crown Court for a binding "overseas production order" if a "designated international cooperation agreement" exists with the recipient's home jurisdiction. The Agreement will make both laws operational between the U.S. and the U.K.

Safeguards. Although the Agreement has not yet been published, official press releases indicate that any request for evidence will be subject to independent judicial oversight or review (usually by a judge or magistrate) of the requesting state, as mandated under national legislation. Both governments also agreed that neither can target "residents" of the other country (without specifying whether that applies to individuals, corporates, or both).

---

[1] The text of the Agreement has not yet been published. For press releases, *see* https://www.gov.uk/government/news/uk-and-us-sign-landmark-data-access-agreement (U.K.) and https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists (U.S.).

The Agreement also bars the use of requested data in prosecutions relating to an "essential interest" of the U.K. or the U.S.—specifically cases implicating freedom of speech if the evidence is requested by the U.K. and death penalty prosecutions if the evidence is requested by the U.S.

Impact. The majority of businesses are unlikely to be on the receiving end of requests under the Agreement. But those that are should prepare to comply with the new scheme. In most cases, this will mean updating internal subpoena and law enforcement request compliance programmes to be able to comply with the shorter time frames for production under the new regime.

For those subject to investigation by U.S. or U.K. authorities, the impact can be significant. Evidence against them could be gathered more quickly than before if held by a service provider in the other jurisdiction. The Agreement also has the potential to impact the manner in which the U.K. Serious Fraud Office conducts cross-border investigations by creating easier and faster access to e-mails and other electronic material, particularly in relation to an uncooperative target or witness.

For U.K.-based companies, the Agreement also goes some way to easing tensions between the CLOUD Act and the EU General Data Protection Regulation ("GDPR"). In July 2019, the European authorities opined that, without an international agreement making a CLOUD Act warrant enforceable, transfer of personal data from the EU to the U.S. pursuant to such a warrant could breach the GDPR. The opinion expressly reserved the position on whether a bilateral agreement under the CLOUD Act, such as the present Agreement, would satisfy the cross-border transfer requirements of the GDPR, though the opinion's language suggests that it would. Of course, companies producing documents would still need to abide by all other GDPR principles, including data minimisation. The rest of the EU would need to await the outcome of the U.S.-EU negotiations of a similar agreement, which commenced on 25 September 2019.

Conclusion. The Agreement will enhance U.S. and U.K. authorities' data gathering arsenal, but the challenges posed by increasingly prevalent use of encryption remain. Upon signing the Agreement, U.S., U.K. and Australian governments published an open letter to Facebook outlining their concerns with its plans to implement end-to-end encryption across its messaging services. They urged Facebook to halt those plans unless and until it enables law enforcement to access content with a warrant in "exceptional circumstances" to tackle serious crimes. It remains to be seen how Facebook and other social media companies will respond to these recurring demands.

Jeremy Feigelson
Partner, New York
+1 212 909 6230
jfeigelson@debevoise.com

Karolos Seeger
Partner, London
+44 20 7786 9042
kseeger@debevoise.com

Jane Shvets
Partner, London and New York
+44 20 7786 9163
+1 212 909 6573
jshvets@debevoise.com

Robin Lööf
International Counsel, London and Paris
+44 20 7786 5447
+33 1 40 73 12 12
rloof@debevoise.com

Robert Maddox
Associate, London
+44 20 7786 5407
rmaddox@debevoise.com

Alma M. Mozetič
Associate, London
+44 20 7786 5449
amozetic@debevoise.com