Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Time To Prepare For New US-UK Data Sharing Rules

By **Omar Shah, Mark Krotoski and Jessica Rogers** (April 29, 2020, 5:34 PM EDT)

Omar Shah

Mark Krotoski

Jessica Rogers

The U.S. and the U.K. have made a historic move in entering into the U.S.-U.K. Bilateral Data Access Agreement. As noted in early February by the head of the Criminal Division of the U.S. Department of Justice, the bilateral agreement reflects law enforcement efforts "to develop mechanisms to address the fact that evidence today is often located overseas."[1]

This landmark agreement, expected to take effect in July, will allow both countries to access electronic data for the purpose of aiding criminal investigations. Despite initial questions regarding the potential impact on individuals' privacy in the U.K. and U.S., the bilateral agreement seeks to balance the interests of law enforcement with the rights of individual citizens.

This article provides an overview of the bilateral agreement to help companies prepare for the new rules providing for the collection of electronic evidence from electronic communication service providers. The bilateral agreement adopted by the U.S. and U.K. is expected to be used as a model for similar agreements with other countries.

The Landscape Before the Bilateral Agreement

The bilateral agreement was signed by the U.S. and U.K. on Oct. 3, 2019.[2] It is the first executive agreement signed under the U.S. Clarifying Lawful Overseas Use of Data Act 2018, or the CLOUD Act, and the U.K. Crime (Overseas Production Orders) Act 2019, or the COPO Act. The acts gave their respective law enforcement agencies the power to issue or apply for warrants, subpoenas or court orders to overseas electronic communication service providers to obtain communications data to aid certain criminal investigations, provided that there is a valid international cooperation arrangement with the overseas country.

The passing of the acts was designed to address the slow, cumbersome and complex mutual legal assistance treaty, or MLAT, process.[3] Under the MLAT process, the time to receive the requested data can be "typically a year but can be years."[4] This attracted considerable public criticism in a recent U.K. criminal investigation into the murder of a teenage girl when the U.K. police were unable to access the suspected murderer's social media account (which held critical evidence) during their investigation.

In the U.K., given that the majority of electronic communication providers hold their data in the U.S., it was hoped that the passing of the COPO Act represented an opportunity for law enforcement agencies to access much-needed data relevant to U.K. criminal investigations.

For the U.S., the enactment of the CLOUD Act also represented an opportunity to clarify the scope of the Stored Communications Act 1986, or the SCA. The U.S. government had challenged a ruling by the U.S. Court of Appeals for the Second Circuit in Microsoft Corp. v. United States where the appellate court found that search warrants issued under the SCA did not have extraterritorial effect.[5]

While the case was pending before the U.S. Supreme Court, the CLOUD Act was enacted and it clarified that the SCA required electronic communication service providers[6] to comply with a U.S. law enforcement warrant or order to provide data within its "possession, custody, or control" even when that data is "located ... outside the United States."[7]

The CLOUD Act also allows for adoption of "executive agreements" providing for law enforcement agencies to have reciprocal access to data maintained in each other's countries in the criminal investigation of serious crimes where minimum protections for privacy and civil liberties are met.

However, implementation of the European Union's General Data Protection Regulation in May 2018 imposed significant constraints on a communication provider's ability to comply with orders issued under the SCA (as amended by the CLOUD Act). The European Data Protection Board and the European Data Protection Supervisor went as far as to conclude that only in very limited cases could an EU provider respond to a SCA order with respect to personal data stored in the EU.[8]

Unless there was a threat to life or physical harm, an EU provider responding to a SCA order may be in breach of the GDPR and subject to fines of €20 million or 4% of global turnover. Similarly, U.S.-based providers were restricted under the SCA from disclosing electronic communications data unless the country in question had a signed agreement with the U.S. complying with the CLOUD Act requirements.

The coming into force of the bilateral agreement will address these issues.

Addressing Privacy and Other Concerns

Despite presenting an opportunity for greater cross-border collaboration and faster criminal investigations, the bilateral agreement has been subject to negative publicity citing concerns over infringement of individual privacy and civil liberties.

In this regard, there are a number of safeguards built into both the bilateral agreement and the acts that seek to strike a balance between aiding law enforcement agencies and protecting individual rights to privacy.

The key safeguards and parameters under the bilateral agreement and acts include:

Scope

Under the bilateral agreement, only data relating to serious crimes (defined as crimes punishable by three years' imprisonment or more) can be requested.[9]

Similarly, requests can only be made to electronic communication service providers, referred to here as covered providers.[10] These are defined as entities that provide communication, processing or storage of data by means of a computer or telecommunications system to the public, or a person processing data on behalf of such an entity. Entities that fall outside this definition are not subject to data disclosure requests under the bilateral agreement (but may be caught by other domestic legislation).

Oversight

Requests for data must be made in accordance with the legislation of the requesting country and subject to independent review by a designated authority. In the U.K., a request made under the COPO Act will be reviewed by a judge who must be satisfied that there are "reasonable grounds" for believing that all or part of the data is likely to be of substantial value to the proceedings or investigation and that it is likely to be relevant evidence with respect to an indictable offence.

There must also be reasonable grounds for believing that it is in the public interest for the data to be accessed by investigators.[11] The "designated authority" for the U.K. is the home secretary, who must review each request and sign a written declaration as to lawfulness.

Similarly, data requests by U.S. enforcement agencies must comply with the process under the SCA, which requires law enforcement agencies to obtain a court order, subpoena or search warrant under judicial scrutiny. The "designated authority" for the United States is the U.S. attorney general, who like the U.K. home secretary, must sign a declaration as to lawfulness of the data request.

Right to Object

Covered providers have the right to lodge a formal objection to a disclosure request with the requesting party and then with their home government.[12] The communication provider's home government may block the disclosure. If the home government declines to do so, the communication provider may challenge this decision using usual domestic avenues (such as judicial review in the U.K.).

Restrictions on Use of Data

Data accessed under the bilateral agreement may not be used for certain types of prosecutions unless the other country has approved its use. For example, the U.K. must give its permission for data accessed under the bilateral agreement to be used in U.S. death penalty prosecutions, and vice versa in relation to U.K. cases infringing U.S. concepts of freedom of speech.[13]

Exclusion of U.K. and U.S. Nationals

U.K. law enforcement agencies may not access data about U.S. nationals, and U.S. law enforcement agencies cannot access data about individuals based in the U.K.[14] However, U.S. agencies may access data about U.K. nationals who are outside the U.K. This difference results from the U.K.'s obligations under EU law, which prohibits different treatment of citizens from different member states.

The U.K. was therefore unable to introduce a prohibition on the targeting of U.K. nationals and instead had to adopt a prohibition on targeting "persons located in the U.K.," which falls short of the protection granted to U.S. nationals (who cannot be targeted regardless of where they are). This position may be revisited after the end of the transitional period depending on what is negotiated with the EU and the timing of the execution of the bilateral agreement.

Notification Requirement With Respect to Individual in a Third Country

With respect to data relating to an individual in a third country, the government of the third country must be notified and given an opportunity to respond (unless to do so would be detrimental to security, impede the investigation, or endanger human rights).[15]

Transparency

Both the U.S. and U.K. must issue an annual report reflecting aggregate data concerning the use of the request mechanism under the bilateral agreement.[16]

No Restrictions on Encryption

Importantly, the bilateral agreement does not require communication providers to provide data in a legible format or de-encrypt data.

What This Means for Electronic Communication Providers

In relation to providers that store data in the U.K., the bilateral agreement acts as a legally binding and enforceable instrument permitting transfer of personal data to the U.S. under Article 46(2)(a) of the GDPR. It is also likely that disclosure will be permitted under the legal basis of "legitimate interest" under Article 6(1)(f) of the GDPR in light of the fact that the purpose of disclosure is to prevent and detect serious crime, and disclosure is governed by a formal international framework that contains a number of safeguards.

As the bilateral agreement satisfies one of the exceptions in the SCA permitting disclosure (because the bilateral agreement constitutes an agreement between the U.S. and U.K., which satisfies the requirements set out in the CLOUD Act), U.S. providers may lawfully respond to U.K. law enforcement requests.

In practice, as the majority of providers store their data in the U.S., the impact of the bilateral agreement is more likely to be felt by such providers. In particular, it is expected that the number of disclosure requests coming from the U.K. to U.S. providers will outstrip the number of requests coming from the U.S.

Given the relative ease of the process under the bilateral agreement and the reduced time frame compared to the MLAT process, it is likely that the volume of international requests will increase, thus creating an increased burden for providers in responding to them.

More broadly, the signing of the bilateral agreement is indicative of the growing trend toward global law enforcement cooperation. In a time of uncertainty for the U.K. in the wake of Brexit, the bilateral agreement will likely provide some comfort to law enforcement authorities that the U.K. will continue to develop mechanisms to share information in cross-border criminal investigations.

Next Steps

The bilateral agreement is subject to a six-month U.S. congressional review period stipulated by the CLOUD Act, ratification by the U.K. Parliament, and designation of the agreement by the U.K. secretary

of state. Provided that approval by both legislative bodies is given, the agreement is expected to come into force in July.[17]

The bilateral agreement will also serve an important role as a model for other countries to enter into similar agreements under the CLOUD Act and the COPO Act. The U.S. and EU announced in September of last year that they had commenced negotiations for a data access agreement,[18] and the following month, a similar announcement was made by Australia and the U.S.[19] The U.K. and EU may negotiate an agreement as part of their broader trade negotiations during the course of 2020.[20]

Omar Shah and Mark Krotoski are partners and Jessica Rogers is an associate at Morgan Lewis & Bockius LLP.

[1] Remarks of Assistant Attorney General Brian A. Benczkowski, U.S. Dep't of Justice, "Justice in Cyberspace" Symposium, Washington, DC (Feb. 5, 2020).

[2] Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime (Oct. 2019); see also Press Release, U.S. Dep't of Justice, U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online (Oct. 3, 2019).

[3] See by way of background
e.g. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/438326/Special_Envoy_work_summary_final_for_CO_website.pdf.

[4] Explanatory Memorandum to the Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, at 1.

[5] See United States v. Microsoft, 138 S. Ct. 1186 (April 17, 2018) (per curiam) (vacating judgment and directing dismissal of the case). For a summary of the decision, see Decision Holds That Search Warrant Cannot Compel Data Stored Overseas (July 15, 2016).

[6] For example, in the U.S., requests for disclosure of data may be made only to providers of "remote computing service[s]," or RCS, and "electronic communication service[s]," or ECS. See 18 U.S.C. § 2510(15) (defining "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications"); id. § 2711(2) (defining "remote computing service" as "the provision to the public of computer storage and processing services by means of an electronic communications system").

[7] 18 U.S.C. § 2713.

[8] Letter to the Chair of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, (July 10, 2018).

[9] Bilateral Agreement, Article I(14).

[10] Under Bilateral Agreement, Article I(7):

Covered Provider means any private entity to the extent that it:

(i) provides to the public the ability to communicate, or to process or store computer data, by means of a Computer System or a telecommunications system; or

(ii) processes or stores Covered Data on behalf of an entity defined in subsection (i).

[11] Bilateral Agreement, Article 5(1).

[12] Id. Article 5(11); id. Article 10(2).

[13] Id. Article 8(4).

[14] Id. Article 5(10).

[15] Id. Article 5(10).

[16] Id. Article 12(4).

[17] See Supplementary letter conveyed to U.S. Congress in Support of U.S.-U.K. CLOUD Act Agreement (January 16, 2020) (noting "the Department considers July 8, 2020 to be the date upon which the agreement will enter into force, absent the enactment into law of a resolution of disapproval as set forth under the statute"); see also Materials conveyed to U.S. Congress in Support of U.S.-U.K. CLOUD Act Agreement (Dec. 4, 2019).

[18] Joint US-EU Statement on Electronic Evidence Sharing Negotiations (Sept. 26, 2019).

[19] Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton (Oct. 7, 2019).

[20] Political Declaration setting out the framework for the future relationship between the European Union and the United Kingdom, paragraphs 8-10. (Oct. 19, 2019).