Bilateral Data Sharing Agreement Between U.S. and UK Enters into Force; What Does it Mean for TMT Companies?

August 2020

Last fall, the U.S. and UK entered into the first bilateral agreement pursuant to the Clarifying Lawful Overseas Use of Data Act of 2018 (the "Bilateral Agreement").[1] The Bilateral Agreement allows, in some circumstances, the U.S. and the UK to demand electronic data directly from tech companies located in the other country.

The U.S. Congress had until July 8, 2020 to enact a joint resolution of disapproval. It has not, so the Bilateral Agreement is now in effect.[2] What does the Bilateral Agreement mean for technology, media and telecommunications ("TMT") companies? Below, we provide guidance to TMT companies that may be on the receiving end of requests pursuant to the Bilateral Agreement.

Background

The CLOUD Act was enacted in 2018 to amend the Stored Communications Act.[3] The SCA, first enacted in the 1980s is the primary means by which the U.S. government obtains email and other content from internet service providers. The CLOUD Act amended the SCA primarily in two ways to make it easier for U.S. authorities to access overseas data and to foster international cooperation. First, the CLOUD Act clarified the SCA's extraterritorial reach. Second, and most relevant here, the CLOUD Act authorized the Attorney General to enter into executive agreements allowing foreign governments to obtain data stored in the U.S., pursuant to their own foreign legal process, without having to go through U.S. authorities.[4]

Similarly, across the Atlantic, the UK enacted the Crime (Overseas Production Orders) Act (the "COPO Act") on February 12, 2019. The COPO Act likewise allows UK authorities to apply to UK courts to compel a company or individual based *outside* the UK to provide electronic data, pursuant to a "designated international co-operation arrangement."[5]

bakerbotts.com | Confidential | Copyright© 2020 Baker Botts L.L.P.

With both the CLOUD Act and the COPO Act in place, the U.S. and UK entered into the Bilateral Agreement on October 3, 2019. The effect of the CLOUD Act, the COPO Act, and the Bilateral Agreement is to allow, in certain circumstances, the U.S. and the UK to obtain electronic data and communications in each other's country, without having to resort to sometimes time-consuming and cumbersome Mutual Legal Assistance Treaty ("MLAT") requests.

Impact of the Bilateral Agreement

Below, we answer some questions regarding the likely impact of the Bilateral Agreement.

☑ **Who can request data under the Bilateral Agreement?**

Only government authorities, and not private entities. When the UK is the requesting party, a UK judge who must be satisfied there are "reasonable grounds" for believing that all or part of the data requested has a substantial value to the proceedings.[6]

U.S. data requests must comply with process under the SCA by obtaining a warrant, court order, or a subpoena, depending on the type of information requested.[7] Notably, to obtain the content of electronic communications under the SCA (and otherwise), U.S. authorities must generally make a showing of probable cause. Non-content information (such as the identity of the subscriber for an email address) can generally be obtained via subpoena, which does not require probable cause.

Once a request is approved, U.S. authorities can serve domestic legal process *directly* on providers in the UK in accordance with U.S. laws and *vice versa*.[8] Unlike with the MLAT process, there is no need for involvement of the UK Foreign Office or UK law enforcement.

☑ **Who can be subject to an order under the Bilateral Agreement?**

The entities potentially subject to an order under the Agreement are private entities that provide services to the public to communicate, process, or store data electronically.[9]

☑ **Who is going to make more requests, the U.S. or the UK?**

Since more tech and telecommunications companies are based in the U.S. than the UK, it's generally anticipated that the U.S. will be on the receiving end of more requests than the UK.

☑ **What types of data may be requested?**

Note that the Agreement explicitly references for the "interception of wire or electronic communications," (i.e., wiretaps),[10] and not merely the collection of stored electronic data (such as emails) and subscriber information.

☑ **What offenses or causes of action are subject to the CLOUD Agreement?**

The Bilateral Agreement is to be used for the prevention, detection, investigation, or prosecution of "serious crime." A "serious crime"[11] is defined by the Agreement as an offense "that is punishable by a maximum term of imprisonment of at least three years" under the laws of the Issuing Party.[12] It is *not* applicable to strictly civil, administrative, or commercial inquiries.[13]

As such, the Agreement *is* applicable to most criminal fraud offenses under U.S. and UK law.

Further, it bears noting that the Agreement can be used to obtain evidence in connection with the investigation—and not just the prosecution—of serious crime. In addition, grand jury secrecy rules do not apply to most data obtained pursuant to the SCA. As such, it is conceivable, for example, that information obtained by the Department of Justice in a criminal investigation could be shared with a civil regulator, such as the Securities and Exchange Commission, which is investigating the same conduct.

☑ **What restrictions are there on requests under the Bilateral Agreement?**

Among other things, the Bilateral Agreement contains numerous "targeting" restrictions in Article 4. Perhaps most significantly, neither country can use an order pursuant to the Agreement to intentionally target "a Receiving-Party person," which, when the United States, is on the receiving end of a request, includes U.S. citizens, lawful permanent residents, and persons located in the territory of the U.S. Orders also may not infringe upon free speech or target individuals based on characteristics such as race, sex, sexual orientation, religion, ethnicity, or political opinion.[14]

☑ **What should companies do if they believe they receive an improper or incorrect production request?**

The Agreement contains mechanisms service providers can follow to challenge a production order. In the first instance, a U.S. service provider can consult with the "designated authority" in the U.K., the Secretary of State for the Home Department. If the objection is not resolved, the U.S. service provider can apply to the U.S. designated authority—the U.S. Attorney General—who will confer with the U.K. designated authority. Ultimately if an agreement is not reached, the U.S. Attorney General can decide that the Bilateral Agreement was not properly invoked and does not apply the production order at issue.

In addition, the COPO Act allows "any person affected by [a COPO] order" to move in the U.K. courts to "vary" or "revoke" an order. Further, the Bilateral Agreement states that providers "retain otherwise existing rights to raise applicable legal objections to an Order subject to Agreement." Thus, we may see litigation in U.S. courts over whether, and to what extent, U.S. service providers can assert constitutional objections to a U.K. production order.

☑ **What this means going forward and how long will it last?**

U.S. companies can expect to be on the receiving end of requests from UK law enforcement agencies. For companies that are accustomed to receiving SCA requests for emails and other stored data from U.S. authorities, the intake and production process will likely not require large changes. However, requests to intercept electronic communications may involve technical hurdles (including re-routing communications to UK authorities) not previously faced by U.S. providers.

How the Bilateral Agreement actually plays out in practice, and how long it lasts, remains to be seen. The Bilateral Agreement provides for review of implementation by the U.S. and UK within the year and mandates that each party's Designating Authority issue an annual report reflecting aggregate data of its use of the Bilateral Agreement.[15] Further, the Bilateral Agreement contains a sunset five years from now, unless the parties agree to extend it. [16]

Neil Coulson
Partner
T: +44.20.7726.3478
neil.coulson@bakerbotts.com

Brendan F. Quigley
Partner
T: +1.212.408.2520
brendan.quigley@bakerbotts.com

Laura Santos-Bishop
Associate
T: +1.212.408.2654
laura.santos-bishop@bakerbotts.com

[1] 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) [hereinafter Bilateral Agreement], see also Press Release, U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online, available at https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists.

[2] See Federal Register, Clarifying Lawful Overseas Use of Data Act; Attorney General Certification and Determination, March 3, 2020, available at https://www.federalregister.gov/documents/2020/03/03/2020-04248/clarifying-lawful-overseas-use-of-data-act-attorney-general-certification-and-determination.

[3] 18 U.S.C. § 2703.

[4] See 18 U.S.C. § 2523

[5] House of Lords Library Briefing: Crime (Overseas Production Orders) Bill [HL], 5 July 2018; Crime (Overseas Production Orders) Act 2019, c. 5, *available at* http://www.legislation.gov.uk/ukpga/2019/5/enacted/data.htm (Accessed: 9 July 2020) [hereinafter COPO Act].

[6] COPO Act (4)(2).

[7] 18 U.S. Code § 2703 (b)

[8] Bilateral Agreement, Article 5 (5).

[9] Bilateral Agreement, Article 1 (7).

[10] Bilateral Agreement, Article 5((3).

[11] Bilateral Agreement, Article 1

[12] Bilateral Agreement, Article 1 (5), (14)

[13] *See* Department of Justice, The Purpose and Impact of the CLOUD Act – FAQs, *available* at https://www.justice.gov/dag/page/file/1153466/download (last visited July 8, 2020).

[14] Bilateral Agreement, Article 4

[15] Bilateral Agreement, Article 12.

[16] Bilateral Agreement, Article 17.