The Computer & Internet Lawyer

Volume 40 ▲ Number 3 ▲ March 2023

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Gathering CLOUD Requests Forecast for Technology and Communications Service Providers

By Robert S. Litt, Patrick E. McDonnell and James McDevitt

As a result of a recent agreement between the United Kingdom and United States, technology and communications service providers should prepare for changes in the landscape of data access requests by UK and U.S. law enforcement agencies.

The U.S. Department of Justice (DOJ) recently announced[1] the entry into force, as of October 3, 2022, of a bilateral agreement between the United Kingdom and United States on Access to Electronic Data for the Purpose of Countering Serious Crime (the UK CLOUD Agreement), which is authorized in the United States under the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act).

The UK CLOUD Agreement will enable law enforcement agencies in either country (through the DOJ's Office of International Affairs and UK Home Office's Investigatory Powers Unit) to access data held by electronic communications or remote computing service providers (such as social media, messaging platforms, and cloud service providers) (collectively, Service Providers) in the other country, for the purpose of combatting serious crime.

The authors, attorneys with Morrison & Foerster LLP, may be contacted at rlitt@mofo.com, pmcdonnell@mofo.com and jmcdevitt@mofo.com, respectively. Harry Anderson, a trainee solicitor at the firm, contributed to the preparation of this article.

WHY WAS THE CLOUD ACT ENACTED?

The CLOUD Act was passed by the U.S. Congress in 2018 to address two issues arising from the Stored Communications Act (SCA)[2] regarding the production of data to law enforcement agencies, namely:

1. *Where foreign law enforcement agencies request data that the United States prohibits Service Providers from producing.*

   The SCA generally prohibits Service Providers from disclosing the content of communications or data about communications, except as authorized by the SCA. The SCA prescribes specific means by which law enforcement agencies can obtain various kinds of data; for example, authorities can obtain the content of stored electronic communications with a warrant issued by a court. However, this applies only to requests from *U.S.* law enforcement agencies; it does not apply to foreign law enforcement agencies. Foreign law enforcement agencies would therefore

need to invoke the cumbersome and time-consuming mutual legal assistance treaty (MLAT) procedures.

2. *Where U.S. law enforcement agencies request data from Service Providers that a foreign country prohibits Service Providers from producing.*

   Following a decision of the U.S. Court of Appeals for the Second Circuit,[3] it became unclear whether a U.S. agency could compel U.S.-based Service Providers to produce data stored outside the United States, pursuant to an SCA warrant.

Both issues led to potentially untenable conflicts of laws. On the one hand, for example, a U.S.-based Service Provider doing business in a foreign country could be subject to both foreign requirements to produce data and the SCA's prohibition on producing that data. On the other hand, U.S. agencies might serve a warrant on a U.S.-based Service Provider calling for production of data located in a foreign country which might have a statute blocking production of such data.

The CLOUD Act addresses these issues by:

- Amending the SCA to authorize the United States to enter into executive agreements with other countries to resolve any potential conflicts of laws. A foreign country that has an executive agreement in place can serve process on a U.S. company under its own laws and the U.S. company is relieved of the prohibition under the SCA. Before the United States can enter into an executive agreement under the CLOUD Act, the U.S. Attorney General, with the concurrence of the Secretary of State, must certify to the U.S. Congress that the partner country has in its law, and implements in practice, robust substantive and procedural protections for privacy and civil liberties. This certification is based on multiple factors, including adequate substantive and procedural laws on cybercrime and electronic evidence, respect for the rule of law and principles of non-discrimination, and adherence to applicable international human rights obligations and commitments.

  At present, the United States has entered into executive agreements with the United Kingdom and Australia. The agreement with Australia was signed[4] in December 2021 and is pending congressional and parliamentary review. We provide further details of the UK CLOUD Agreement below.

- Confirming that, pursuant to the SCA, U.S. authorities can compel Service Providers to produce data, including the contents of communications, wherever it may be located, pursuant to the procedures authorized by the SCA.

HOW WILL THE UK CLOUD AGREEMENT IMPACT SERVICE PROVIDERS?

Upon the request of law enforcement agencies, Service Providers may be required to preserve, back up, or disclose data to the agencies for the purposes of the prevention, detection, investigation, or prosecution of serious crime, including terrorism, sexual exploitation of children, and cybercrime.

The UK CLOUD Agreement enables law enforcement agencies of either country to make requests directly to Service Providers in the other country (Requests), provided the requirements in the UK CLOUD Agreement are satisfied (as summarized below). Previously, law enforcement requests would have to go through the MLAT process.

The UK CLOUD Agreement, in turn, also removes barriers under U.S. domestic law (as noted above) which previously prohibited Service Providers from responding to law enforcement agencies of the other country to disclose electronic data.

WHAT ARE THE KEY LIMITATIONS AND REQUIREMENTS UNDER THE UK CLOUD AGREEMENT?

The scope of the CLOUD Act and UK CLOUD Agreement is limited to Service Providers (i.e., those entities which are subject to the SCA restrictions described above). All other organizations are therefore unaffected by this regime. Furthermore, the CLOUD Act and UK CLOUD Agreement only concern access to data by law enforcement. As such, the CLOUD Act regime does not affect access to data for national security purposes.

Furthermore, we should note that the CLOUD Act does not give either the United States or any foreign country additional bases to seek data, which would still be governed by the laws of the requesting country.

However, the UK CLOUD Agreement includes specific requirements that must be met for the U.S. or UK law enforcement agencies to issue Requests, including that:

1. A law enforcement agency of one country must not intentionally target companies registered in the other country or other persons located in the other country;

2. Requests must relate to a serious crime (i.e., crimes that are punishable with a maximum term of imprisonment of at least three years);

3. Requests may not be used to infringe freedom of speech or for disadvantaging persons based on their race, sex, sexual orientation, religion, ethnic origin, or political opinions; and

4. Requests must relate to the following types of data held or processed by Service Providers: (a) the content of an electronic or wire communication; (b) computer data stored or processed for a user; (c) traffic data or metadata pertaining to an electronic or wire communication or the storage or processing of computer data for a user; or (d) subscriber information.

WHAT ARE THE KEY CONSIDERATIONS FOR SERVICE PROVIDERS?

Service Providers are not compelled to decrypt the data requested by law enforcement agencies. Furthermore, the UK CLOUD Agreement also permits a Service Provider to raise specific objections when it has a reasonable belief that the UK CLOUD Agreement may not be properly invoked. Any objections should be raised by a Service Provider to the law enforcement agency issuing the Request within a reasonable time after its receipt. If the objections are not resolved, the Service Provider may thereafter raise objections with its domestic law enforcement agency. The two agencies may then work together to resolve the objections. However, if the Service Provider's domestic law enforcement agency concludes that the UK CLOUD Agreement was not properly invoked, the UK CLOUD Agreement will not apply to the Request.

Service Providers will also be expected to respond to Requests in a much shorter timeframe under the UK CLOUD Agreement, namely in a matter of weeks, rather than months, as is commonplace under the MLAT process. Any actions taken in the event of non-compliance will be governed by the legislation of the country of the law enforcement agency making the Request.

WHAT'S ON THE HORIZON?

The CLOUD Act aims to deal with the multi-jurisdictional nature of electronic data and avoid problems of data localization through bilateral negotiations. As criminal investigations become ever more global, we expect that more countries will have a strong incentive to increase ways to permit data flows across borders to assist in law enforcement investigations.

To that end, in addition to the United Kingdom and Australia, the United States has already started further CLOUD Act agreement negotiations with Canada[5] and the European Union.[6] The EU negotiations, however, are likely to be more protracted than others. This is primarily because the EU will need to resolve its own internal e-evidence rules and because it does not have a single law enforcement agency. EU Member States would therefore need to make their own data requests, some of which may not meet U.S. due process standards.

Notes

1. https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force.
2. 18 U.S.C. §§ 2701-2713.
3. Microsoft v. United States, No. 14-2985 (2d Cir. 2016).
4. https://www.justice.gov/opa/pr/united-states-and-australia-enter-cloud-act-agreement-facilitate-investigations-serious-crime.
5. https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement.
6. https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations.