THE CLOUD ACT

Last update: 22/12/2022

1. BACKGROUND

The importance for public authorities of accessing electronic evidence (e-evidence) held by Online Service Providers (OSPs) in criminal investigations has been growing in recent years, and with it the need for facilitating and accelerating this process for all the parties involved. Domestic authorities all around the world are facing multiple challenges in acquiring such evidence, some of which have also been the driving factors behind the 2018 changes in the U.S. legislation:

a) Several OSPs with offices and customers all over the world hold electronic data in **servers located abroad**, sometimes **in multiple countries**, constantly and automatically moving it across borders. With the technology developments (e.g. cloud services) and the borderless nature of internet, **obtaining data** (via voluntary or mandatory cooperation channels) in criminal investigations is becoming increasingly challenging for the investigating authorities and sometimes for the OSPs themselves. The territoriality concept in the context of electronic data acquisition was at issue also in the controversial Microsoft-Ireland case, in which a U.S. court held in 2016 that the Stored Communications Act (SCA) did not authorize the U.S. government to require disclosure of data stored abroad (Ireland) from a company subject to U.S. jurisdiction.[1]

b) Some of the **largest OSPs holding relevant e-evidence operate under the U.S. jurisdiction**.[2] With the growing number of Mutual Legal Assistance (MLA) requests seeking access to e-evidence held by the U.S.-based OSPs (often the only link of a foreign criminal investigation with the U.S.)[3], the U.S. has been struggling with providing **timely assistance to foreign partners** under the existing MLA process.[4]

When applying the Agreement on MLA between the EU and the U.S. in practice, the judicial authorities of the EU Member States have repeatedly identified the length of the procedures as the main problem they have encountered when addressing **MLA requests** at the U.S. authorities.[5]

c) Adding to the complexity of accessing e-evidence in a timely and efficient manner is the fact that the **OSPs and the data they control may be subject to more than one country's laws** which can present conflicting obligations for the OSPs faced with an order to produce electronic data.

Against this background, on 23 March 2018, the U.S. Congress adopted the **Clarifying Lawful Overseas Use of Data Act** (CLOUD Act).

> "The CLOUD Act is an important step in our efforts to minimize the challenges we all face in obtaining access to electronic evidence stored outside our borders."[6]

2. THE SCOPE

- **Legal regime covered**

The purpose of the CLOUD Act was to improve procedures for both the U.S. and foreign authorities in obtaining access to data held by OSPs in the context of criminal investigations. This twofold purpose was reflected in the structure of the Act, which is comprised of **two main parts**.

[1] The 2016 decision was challenged before the Supreme Court.

[2] COM, Recommendation for a Council decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters Available at : EUR-Lex - 52019PC0070 - EN - EUR-Lex (europa.eu).

[3] Ibid; and U.S. DoJ, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, White Paper (April 2019).

[4] Deputy Assistant Attorney General Richard W. Downing, *What the U.S. Cloud Act Does and Does Not Do* (May 2019).

[5] SIRIUS EU Digital Evidence Situation Report, December, 2022, p. 48. 89% of the respondents to a survey among EU Member States' judicial authorities indicated length, 40% interpretation of a violation of freedom of speech and 25% difficulties in drafting the MLA requests including probable cause. The length of the MLA process was also pinpointed by law enforcement authorities as one of the main challenges when dealing with requests to foreign-based OSPs.

[6] Deputy Assistant Attorney General Richard W. Downing, *What the U.S. Cloud Act Does and Does Not Do* (May 2019).

The SIRIUS project has received funding from the European Commission's Service for Foreign Policy (FPI) under contribution agreement No PI/2020/417-500. This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

Firstly, influenced by the Microsoft-Ireland case, the Act removed any doubts as to the extraterritorial effect of the probable cause warrants issued under the SCA, by making explicit the **obligation of the U.S. service providers to preserve and produce data they control regardless of where it is stored**.[7]

Secondly, and more importantly for the EU authorities, the Act authorized the U.S. to enter into "**executive agreements**" with foreign governments, removing restrictions under each country's law so that service providers based in one country can comply with direct orders for disclosure of electronic data issued by another country. In this context, the CLOUD Act allowed the U.S.-based service providers to **disclose the content of communications directly in response to a foreign government's order** with a CLOUD Act executive agreement in place.[8]

The first executive agreement under the CLOUD Act was signed with the **UK** in October 2019 and entered into force on 3 October 2022.[9]

Following formal negotiations, the US and **Australia** signed the CLOUD Act executive agreement in December 2021 (the date of its entry into force is still unknown).

- **Data covered**

The CLOUD Act executive agreements may, **depending on the agreement of the parties,** cover access to **stored content and non-content data** (any record or other information pertaining to a customer or subscriber of a provider) as well as **real time interception of communications**.[10] According to the U.S.-UK executive agreement, for example, the following types of data are covered by the orders issued pursuant to the agreement when possessed or controlled by a service provider:

> "Content of an electronic or wire communication; computer data stored or processed for a user; traffic data or metadata pertaining to an electronic or wire communication or the storage or processing of computer data for a user; and Subscriber Information when sought pursuant to an Order that also seeks any of the other types of data referenced in this definition."[11]

The CLOUD Act executive agreements may determine explicitly the kind of orders that can be issued directly to the service providers and the type of data they cover. Therefore, they could potentially go significantly beyond the data types covered by the Second Additional Protocol to the Budapest Convention on Cybercrime[12] and the e-evidence legislative package proposal[13], in particular with respect to the real-time interception of communications.

As specifically stipulated already in the CLOUD Act, foreign government orders issued under the executive agreements may not intentionally **target data of U.S. persons** or persons located therein, nor can they target non-U.S. persons located outside the U.S. for the purpose of obtaining information about a U.S. person or a person located therein.[14] Any reciprocal limitation on the U.S. authorities with respect to foreign citizens and/or residents is subject to negotiations of the executive agreement.[15]

- **Types of crimes covered**

An order subject to a CLOUD Act executive agreement may only relate to information needed for the prevention, detection, investigation, or prosecution of "**serious crime**".[16] What constitutes a serious crime is not further defined in the Act, apart from the fact that the term includes terrorism. It is thus left to the Parties to the executive agreement to define the exact scope of the term.[17]

[7] See, White Paper, p. 7.
[8] Sec. 104(j) of the CLOUD Act.
[9] *UK/USA: Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime [CS USA No.6/2019] - GOV.UK (www.gov.uk); Joint Statement by the United States and the United Kingdom on Data Access Agreement | OPA | Department of Justice* (July 2022).
[10] *The Purpose and Impact of the CLOUD Act - FAQs*. Deputy Assistant Attorney General Richard W. Downing, *What the U.S. Cloud Act Does and Does Not Do* (May 2019).
[11] Article 1(3) of the U.S.-UK Agreement. The same provision is included in the *U.S.-Australia executive agreement* (Article 1(4)).
[12] The Protocol does not contain provision for obtaining content or traffic data directly from a foreign service provider, nor does it includes provisions on acquisition of intercepted communication.
[13] The proposal does not cover real-time interception of telecommunications. For additional information, see the related factsheets available on the SIRIUS platform here.
[14] Sec. 105 of the CLOUD Act.
[15] According to the U.S.-UK executive agreement, for example, orders cannot target citizens of the Parties and the companies incorporated in the Parties' territories. UK citizens are protected only when they are in the UK, while U.S. citizens are protected when they are abroad as well. According to the U.S.-Australia executive agreement, the reciprocal limitation applies as the orders cannot target citizens of either Party regardless of their location.
[16] Sec. 105 of the CLOUD Act.
[17] The U.S.-UK executive agreement, for example, defines "serious crime" as an offence punishable by maximum three

- **Service providers covered**

The CLOUD Act concerns providers of "**electronic communication service[s]**"[18] and "**remote computing service[s]**"[19].

CLOUD Act executive agreements do not, by themselves, extend jurisdiction of the State Party to the agreement over any foreign service provider that cannot be compelled to produce data **under that State Party's domestic law**.[20] The U.S. authorities can, for example, issue SCA warrants only to the service providers subject to the U.S. jurisdiction as determined by the SCA and CLOUD Act, regardless of where the data is stored.[21] However, the reach of the CLOUD Act does not end with the providers headquartered in the U.S., but includes those operating with or in the U.S. Moreover, any EU entity, including EU institutions, that uses services which have a direct or indirect corporate link with the U.S. could fall under the extraterritorial reach of the CLOUD Act.[22]

3. DEFINING THE TOOLBOX

The CLOUD Act provides an alternative framework to the conventional judicial cooperation channels. It establishes the possibility of adoption of **executive agreements** with foreign governments, which serve as a lawful mechanism (removing legal barriers) for either of the Parties to the agreement to request (order) data **directly from a service provider** located within the jurisdiction of the other Party. Orders issued under such executive agreements must be consistent with domestic law, as well as the law of the other Party, without the need to go through the MLA process. Such agreements are aimed at resolving **conflicts of law** that may arise in situations where service providers served with preservation and production orders are bound by conflicting legal obligations of the countries concerned (i.e. foreign government orders for production of electronic data that U.S. may prohibit providers from disclosing and *vice versa*).[23]

In order to be able to conclude the executive agreement with the U.S., the foreign government has to fulfil certain CLOUD Act requirements related to **substantive and procedural protections for privacy and civil liberties in that country**.[24] Recognising the significance of the existing international legal framework on cross-border access to e-evidence, the foreign government's adherence to the requirement of having adequate substantive and procedural laws on cybercrime and e-evidence can be, *inter alia*, demonstrated by it being a party to the *Budapest Convention on Cybercrime*.

Following the two executive agreements under the CLOUD Act the U.S. have already concluded with the UK and Australia, **Canada** and the U.S. have entered into formal negotiations on a CLOUD Act executive agreement in March 2022.

On 25 September 2019, the **EU** and the U.S. officially started to negotiate an agreement on cross-border access to e-evidence for judicial cooperation in criminal matters.

> "We need to work together with our American partners to speed up the access of our enforcement authorities to this evidence. This will strengthen our security, while protecting the data privacy and procedural safeguards of our citizens. The launch of negotiations marks an important step towards achieving this."[25]

The architecture of such an agreement (e.g. a self-standing EU-wide agreement or an EU-U.S. umbrella agreement followed by bilateral agreements by the Member States) remains unclear.[26]

4. ISSUING PARTY

years (Article 1(14)). The U.S.-Australia executive agreement provides the same definition (Article 1(15)).

[18] See definition in 18 U.S.C. § 2510(15).

[19] See definition in 18 U.S.C. § 2711(2).

[20] Sec. 105 of the CLOUD Act: "[a]ny obligation for a provider … to produce data shall derive solely from that law…"

[21] See changes introduced in the UK and Australian domestic legislation, allowing for an international production order that the UK and Australian authorities respectively can serve directly on the foreign service providers.

[22] EDPS, September Newsletter (96), 30 September 2022. Available at: Newsletter | European Data Protection Supervisor (europa.eu).

[23] The CLOUD Act, pp. 2021, 2023.

[24] It has to, for example, have adequate laws on cybercrime and e-evidence, respect for the rule of law and human rights, clear legal mandates and procedures governing the collection, retention, use and sharing of e-data, etc.

[25] European Commissioner for Justice, Věra Jourová, *Joint US-EU Statement on Electronic Evidence Sharing Negotiations* (September 2019).

[26] See, T. Christakis and F. Terpan, "EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options", *International Data Privacy* Law, pp. 81-106, April 2021.

Although the term "Issuing Party" is not present in the CLOUD Act, it can be found in both, the "U.S.-UK Data Access Agreement" and the "U.S.-Australia Data Access Agreement". The term "Issuing Party" refers to the country that issues the request for the preservation or disclosure of data directly to the service provider, located in the "Receiving Party" (country where the service provider is located).

A- ISSUING AUTHORITIES

Orders issued by the Issuing Party under the CLOUD Act agreement must be subject to **review or oversight by a court, judge, magistrate or other independent authority**.[27]

B- ISSUING CONDITIONS

- **Domestic law compliance**

The order that is subject to an executive agreement must be issued in compliance with the Issuing Party's **domestic law** for accessing data in question.[28]

- **Specificity, necessity and proportionality**

The order must **identify its object** with a specific identifier, such as the specific person, account, address or personal device targeted.

It must be issued for the purpose of obtaining information relating to the **prevention, detection, investigation, or prosecution** of serious crime.

The order must be **reasonably justified**. In particular, it must be based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation.

The CLOUD Act adds supplementary conditions for issuing **orders for interception of wire or electronic communications**, making the necessity and proportionality assessment more rigorous. In particular, they can only be issued for a fixed duration that may not be longer than what is reasonably necessary to accomplish the approved purposes of the order. In addition, they cannot be issued if the same information could be reasonably obtained by using less intrusive methods.

C- ISSUING PROCEDURE

The Issuing Party may issue orders subject to an executive agreement **directly to the service provider**.

Further details regarding the issuing procedure are subject to the executive agreement itself. According to the U.S.-UK Agreement and the U.S.-Australia Agreement, for example, a specifically designated authority of the Issuing Party must, prior to its transmission, review the order for its compliance with the Agreement, provide a written certification attesting to this fact and its lawfulness, and notify the service provider of invoking the Agreement in relation to a particular order.[29]

D- USE AND ADMISSIBILITY OF DATA OBTAINED

The CLOUD Act includes a specific limitation to the use of the obtained electronic information in case of an infringement of the **freedom of speech**. It stems from the U.S.-U.K. Agreement and the U.S.-Australia Agreement that other limitations to the use and admissibility of the acquired data can be agreed on in the executive agreement itself: UK and Australia, respectively, may oppose to the use of the collected data as evidence in the prosecution of offences in the U.S. for which the death penalty is sought.[30]

5. SERVICE PROVIDERS

CLOUD Act executive agreements do not by themselves impose **any new obligation on non-U.S. based service providers** to comply with a U.S. government order or on U.S.-based service providers to comply with a foreign government order. Any obligation of the service provider to comply must stem from the Issuing Party's domestic law.

- **Challenge of orders**

(i) The service providers must in principle challenge any order subject to an executive agreement in accordance with the **procedure envisaged by the Issuing Party's domestic law**.

(ii) It stems from the U.S.-UK Agreement and the U.S.-Australia Agreement that **executive agreements can (in addition) determine a specific**

[27] Nothing changes as regards the conditions for the U.S. authorities to obtain a warrant for the content of electronic communications under the U.S. law: request to issue a warrant must be submitted to an **independent judge** for approval.

[28] In practical terms, this means that, unless this is required by their domestic laws, the qualifying foreign governments no longer need to comply with the probable cause requirement under the U.S. law in relation to accessing content data held by the U.S.-based service providers.

[29] Article 5(6)(7)(8) of the U.S.-UK Agreement and the U.S.-Australia Agreement.

[30] Article 8(4)(a) of the U.S.-UK Agreement and Article 9(4) of the U.S.-Australia Agreement.

procedure for the service provider to challenge the orders subject to the agreement, including the possibility of bringing the Receiving Party's authorities into the resolution process.[31]

In particular, under those agreements, the service provider which has reasonable belief that the Agreement may not be properly invoked in respect of a particular order, may raise objections to this end first with the Issuing Party's Designated Authority. If the objections are not resolved, the service provider may raise the objections to the Receiving Party's Designated Authority. Both Parties' Designated Authorities may meet to discuss the solution and address any issues raised under the agreement. The final decision on whether the agreement has been properly invoked and, consequently, whether the agreement shall apply to a particular order, lies with the Receiving Party which should properly inform the service provider and the Issuing Party of its (negative) assessment.

(iii) In addition, the CLOUD Act provides for a procedure for service providers to file a **motion to quash or modify** an order issued by the U.S. authorities, where the provider that falls under the U.S. jurisdiction reasonably believes that:

i. the order relates to a customer or subscriber who is not a U.S. person and does not reside in the U.S.; and
ii. the required disclosure would create a material risk that the **provider would violate the laws of a country that has concluded an executive agreement**.[32]

The court may decide to modify or quash the challenged legal order if:

i. the required disclosure would cause the provider to violate the laws of the country that has concluded an executive agreement;
ii. the interests of justice dictate such decision;[33] and
iii. the customer or subscriber is not a U.S. person and does not reside in the U.S.

- **Sanctions**

Orders subject to the executive agreements derive their legally binding nature exclusively from the law of the Issuing Party. Any sanctions for non-compliance of the service provider with such an order are therefore **dependent on the domestic law of the Issuing Party**.

Importantly, the CLOUD Act determines that no cause of action shall lie in any (U.S.) court against the service provider who provided information or other assistance in accordance with an order from a foreign government that is subject to an executive agreement.

6. RECEIVING PARTY

The only law governing enforcement of the orders subject to executive agreements is the law of the Issuing Party which is entitled to obtain electronic data from the service provider in the Receiving Party without its prior approval or oversight.

Pursuant to the CLOUD Act, the U.S., however, reserve the right to render an executive agreement inapplicable as to any order for which the U.S. Government concludes the agreement may not properly be invoked. Similar provisions regarding the role of the Receiving Party stem from the U.S.-UK Agreement and the U.S.-Australia Agreement.[34]

7. CHALLENGES

- **Absence of executive agreements – continued conflicting legal obligations for the service providers**

The first group of challenges regarding the CLOUD Act is related to the fact that even though the CLOUD Act has been enacted more than three years ago, only two executive agreement have been concluded so far (with only one that has already entered into force), making the reach of any provisions of the CLOUD Act on executive agreements framework very limited.

Where the data sought by U.S. authorities is not located in a country with which the U.S. has reached an executive agreement, service provider's obligation to comply with the SCA warrant from the U.S. (with an extraterritorial effect) might conflict with a foreign country's law prohibiting the production of the requested data. This remains an issue within the existing **EU legal framework** and absent an international CLOUD Act agreement between the U.S. and EU: the OSPs controlling personal data whose processing is subject to the

[31] Article 5(11)(12) of the U.S.-UK Agreement and the U.S.-Australia Agreement.
[32] 18 U.S.C. § 2703(h).
[33] Under the comity analysis, the court should, *inter alia*, consider the investigative interests of the U.S. and the interests of the foreign government in preventing disclosure; the likelihood of sanctions for the provider and/or its employees; the location and nationality of the subscriber or customer; provider's link with the U.S., etc.
[34] See Article 5(11)(12) of the U.S.-UK Agreement and the U.S.-Australia Agreement.

General Data Protection Regulation (GDPR) or other EU or Member States' law do not appear to be allowed to respond directly to the law enforcement requests for personal data from the U.S. and lawfully disclose/transfer personal data to the U.S., except in exceptional circumstances where processing is necessary in order to protect the vital interests of an individual whose life or physical integrity is at risk.[35]

If the U.S. authorities decide to pursue the order notwithstanding **conflicting legal obligations for the provider**, the latter only has the right to challenge a SCA warrant under "common law … comity analysis".[36] The success rate of any such challenges following the adoption of the CLOUD Act and the willingness of the service providers to undertake the procedure is unknown. In fear of high financial penalties associated with breaches of GDPR provisions, the service providers seem to have (at least in the past) rejected any such requests submitted directly to them or refer the U.S. authorities to the traditional MLA procedure.[37]

- **Enforcement**

The second group of challenges relates to the enforcement of the production and preservation orders that are subject to the executive agreements. The CLOUD Act **lacks any specific enforcement mechanism**, leaving the enforcement of such orders completely in the hands of the Issuing Party with no foreseen assistance from the Receiving Party in case of non-compliance. Even where the executive agreements are in place, but the service provider does not comply with the production order issued under that agreement, the Issuing Party might therefore still need to seek disclosure of electronic data through the MLA process.[38]

[35] See EDPB and EDPS, *ANNEX. Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence* (July 2019). Amicus Curiae brief of the European Commission in U.S. v. Microsoft Corporation, p. 14.

[36] Sec. 103(c) of the CLOUD Act.

[37] Report of CEPS and QMUL Task Force, *Cross-border data access in criminal proceedings and the future of digital justice*, p. 23.

[38] Since the U.S. law allows U.S.-based service providers to cooperate directly with competent EU authorities with regard to non-content data pertaining to non-US citizens or residents, **voluntary cooperation channels** are another alternative to the MLA process. However, seeking disclosure of data through the latter still remains the only possible venue for the EU Member States if: specific (mainly content) data is necessary for investigation, gathered information would otherwise not be admitted as evidence in the court or the process of voluntary cooperation does not give desired results.