European Parliament
2014-2019

Committee on Civil Liberties, Justice and Home Affairs

11.3.2019

4th WORKING DOCUMENT (B)

on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Relation with third country law

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Birgit Sippel
Co-Author: Sophie in 't Veld

The CLOUD Act also provides for a comity procedure by laying down the modalities for a provider to possibly challenge such an order to produce content located outside the US, based on a conflict of law:

A challenge has to be made within 14 days,
a) if the communication content concerns a foreign person (i.e. not a US citizen or US resident) and,
b) if compliance with the order would create a material risk to violate a third country law.

In order for the third country law to be taken into account, the third country must be considered a "qualifying foreign government" and in order to qualify, the country must have an executive agreement with the US on the issue (see Part II below).

Faced with a challenge, the US government entity that made the original request is provided a possibility in the procedure to respond. The court is permitted (not required) to quash the order:
a) if foreign laws would be violated,
b) if "the interests of justice dictate" such quashing based on "the totality of circumstances",[1] and
c) the individual is a foreign person residing outside the US.[2]

In Part II (§2523), a new section has been added concerning executive agreements with foreign governments regarding access to data stored in the US. Under this section, the President of the United States may enter into an executive agreement with a foreign government, in order to allow providers of electronic communication services to the public or remote computing services to disclose their customers' data stored in the US to such a foreign government. However, this possibility only concerns data of non U.S. persons. For requests for data on U.S. persons, the foreign government will have to use the Mutual Legal Assistance Treaty (MLAT) process or obtain assistance in a criminal investigation or prosecution (28 U.S. Code §1782 and 18 U.S. Code §3512). In addition, a kind of adequacy decision of the mentioned country has to be taken beforehand and reciprocity applies (made by the Attorney General and provided to Congress).[3] Consequently, the CLOUD Act has extra-territorial

[1] For such an assessment the following criteria is used: ''(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure; ''(B) the interests of the qualifying foreign government in preventing any prohibited disclosure; ''(C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider; ''(D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country; ''(E) the nature and extent of the provider's ties to and presence in the United States; ''(F) the importance to the investigation of the information required to be disclosed; ''(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and ''(H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

[2] The Commission proposal of Article 16 models the US Cloud Act procedure.

[3] In that regard the domestic law of the foreign government, including the implementation of that law, must afford robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government. The factors to be met in making such a determination include whether the foreign government: (i) has adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated by being a party to the CoE Convention on Cybercrime, (ii) demonstrates respect for the rule of

consequences and gives access to the data of US citizens and residents, as well as of non US nationals, irrespective of their global location, if they are suspected of an offence for which US authorities have jurisdiction.

Regarding the data sought and the nature of the measure, the measure is considered a national measure and the US authorities have to fully follow the US legislative and constitutional safeguards. From this it follows that content of an electronic communication that is in electronic storage in an electronic communication system for 180 days or less, always requires the issuing of a US warrant. For documents in online cloud storage and records pertaining to a subscriber or a customer, a US court order may be necessary and the government entity shows that there are reasonable grounds to believe that the information sought is "relevant and material to an ongoing criminal investigation". For the disclosure of subscriber information, an administrative subpoena may be used.[4]

2. Compatibility between the CLOUD Act and the EU e-evidence proposal

Based upon the afore presented consequences of the enacted CLOUD Act, there seem to be certain incompatibilities between EU and US legislations which could lead to conflicts of law. First, as regards those service providers based in the US and collecting or storing data in a third country, the CLOUD Act should apply. However, if those providers also offer services in the European Union, they would also be subject of the e-evidence instrument, if adopted, since the Commission proposal stipulates the appointment in the EU of a legal representative of the service provider based in the US. Furthermore, already now, they are subject to the General Data Protection Regulation. Second, in cases where the data to be disclosed are located in the US, the CLOUD Act requires the conclusion of executing agreements, subject to the fulfilment, by the third country concerned, of a number of conditions which are not reciprocal. However, the proposed e-evidence Regulation would allow for the disclosure of data located in the US without any prior conclusion of an executing agreement, and without any consideration of the nationality of the person concerned with the disclosure, as long as the service provider offers services in the EU. Finally, if a service provider raises the issue of conflicting obligations between US and EU laws, it is unclear which review procedure would apply. The CLOUD Act, on the one hand, provides for the possibility for the provider to file a motion to modify or quash the legal process (as regards disclosure of data of non-US citizens not residing in the US) - if an executing agreement between the US government and the EU Member State concerned has been concluded. In case no executing agreement has been concluded, it seems that the disclosure order could be challenged on the basis of common law comity analysis only. The proposed e-Evidence Regulation, on the other hand, provides for two review procedures, irrespective of the nationality of the person concerned and partially allowing for the intervention of the national central authority of this third country (see below Articles 15 and 16 of the draft Regulation).

---

law and principles of non-discrimination; (iii) adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights, (iv) has clear legal mandates and procedures governing those entities of the foreign government that are authorized to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective oversight of these activities; (v) has sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government; and (vi) demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet.

[4] See Stored Communications Act (SCA), codified at 18 U.S.C. Chapter 121 §2703.

EU draft negotiating mandate with the US on e-evidence

On 5 February 2019, the Commission issued the "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".[5]

The Commission justifies its competence with reference to the pending e-evidence Proposal by arguing that "The Commission's e-evidence proposals provide the basis for a coordinated and coherent approach both within the European Union and by the European Union at international level, with due regard to European Union rules, including on non-discrimination between European Union Member States and their nationals". According to the Commission, such a proposal "could usefully be complemented by bilateral or multilateral agreements on cross-border access to electronic evidence with accompanying safeguards" and that "An EU-U.S. Agreement should aim to avoid conflicting obligations between the European Union and the United States of America".

Moreover, after making reference to the CLOUD Act and possible executive agreements between the US authorities and foreign governments, the Commission states that "the purpose of this initiative is to address, through common rules, the specific legal issue of access to content and non-content data held by service providers in the European Union or the United States of America" as well as to "complement the EU's electronic evidence proposals by addressing conflicts of law, in particular as regards content data and speeding up access to electronic evidence". Based on this the Commission itself comes to the conclusion that such an agreement "would offer a number of practical advantages", enumerating, among others, the reciprocal access for judicial authorities to content data as well as to non-content data on the basis of orders from judicial authorities. They claim it would also contribute to improving timely access to data, address the risk of conflicts of laws, and reduce the risk of fragmentation of rules and procedures. Finally, the Commission states that the Agreement would clarify the binding nature and enforcement of orders on service providers while detailing the obligations for judicial authorities.

Such a mandate, however, raises several questions, namely:

- First, the proposed mandate seems to complement a legislative proposal that is still pending.[6] One could even argue that the proposed mandate does not only complement the e-evidence proposal, but would basically be based on it. Thus, the question arises whether the actual intention by the Commission, when presenting the e-evidence proposal, was to get a justification for a legal basis for an international agreement with the US. If the agreement was adopted before the e-evidence proposal, the question would be to know how the agreement would have an impact on the legal system to be established by the e-evidence proposal.

- Second, as mentioned before, the question arises whether such an agreement would be necessary if the option of providing more financial, technical and human resources to judicial authorities both in Member States and in the US handling mutual legal assistance requests has not been fully explored and addressed yet.

[5] COM(2019) 70.
[6] The UK did not opt-in to e-evidence and is negotiating its own agreement with the US under the Cloud Act

- Third, it has to be clarified if and how such an agreement (depending on its status) could be envisaged outside the framework of the CLOUD Act. This questions is particularly important given that the US legislation is very clear as to which data can be requested by foreign authorities (namely only data of non-US citizens and non-residents), whereas, at the same time, the US government can request all data, including data stored or collected outside of the United-States - question of reciprocity of any future agreement.

- Fourth, it also has to be clarified if the EU actually falls under the term "foreign government" and, thus, can conclude such an agreement under the Cloud Act. It has already been claimed that any EU-US e-evidence agreement could be only a framework agreement demanding additional agreements by the individual Member States.[7]

- Finally, one could raise the general question of why such an agreement is necessary if the e-evidence proposal clearly provides provisions regarding access to data stored in third countries and also provides for a comity procedure regarding conflicts of jurisdictions with a third country (see Art. 15 and 16).

Unfortunately, these questions have not been sufficiently answered by the Commission so far.

[7] See J. Daskal and P. Swire, A Possible EU-US Agreement on law enforcement Access to Data?, Lawfare 2018.