**Council of the European Union**

**Brussels, 26 February 2018**
**(OR. en)**

**6339/18**

**LIMITE**

**JAI 126**
**COPEN 42**
**DROIPEN 20**
**CYBER 33**

**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Permanent Representatives Committee/Council |
| Subject: | Improving cross-border access to e-evidence |

1. The Council conclusions of 9 June 2016 on improving criminal justice in cyberspace[1] stressed the importance of e-evidence in criminal proceedings for all types of crimes. They acknowledged the need '***as a matter of priority, to find ways to secure and obtain e-evidence*** *more quickly and effectively by intensifying cooperation with third countries and with service providers that are active on European territory ... and direct contacts with law enforcement authorities and to identify concrete measures to address this complex matter*'. The Commission was requested to take concrete steps in that regard in association with Member States and to report on the progress made.

1 10007/16.

2. Accordingly, the Commission launched a comprehensive expert process, including also representatives of industry and civil society organisations. As envisaged in the 2016 Council conclusions, a mid-term progress report[2] and a final report of the findings[3] were presented to the Council at the end of 2016 and in June 2017. They outlined a number of possible **practical and legislative measures to address the obstacles** faced in criminal investigations in relation to access to e-evidence that is often stored outside the investigating country or handled by a foreign service provider. These measures aimed to overcome the main shortcomings of judicial cooperation mechanisms such as MLA, mutual recognition or voluntary direct cooperation of service providers, which render these mechanisms inadequate to serve the needs of criminal justice today.

3. Those measures were positively received by the Member States, in particular the measures aiming at **establishing a legal framework** authorising competent national authorities to directly request or compel a service provider in another Member State to disclose e-evidence processed in the EU on the basis of certain conditions and safeguards. Such a framework would allow for faster access to e-evidence while ensuring protection of fundamental rights and legal certainty, thereby reducing fragmentation and conflicts of law[4]. The various components of that future legislative proposal were subject to consultations with Member States' experts, service providers and civil society organisations, and the proposal was expected to be officially presented to the Council in the first quarter of 2018[5].

---

**2** 15072/16.
**3** 9554/17.
**4** Commission Inception Impact Assessment (Ares(2017)3896097) of 3 August 2017.
**5** COM(2017) 650 final, Annex I, p. 5.

4. Almost in parallel to the process taking place within the EU, the Council of Europe, on the basis of the Cloud Evidence Group recommendations, decided to draft an **additional protocol to the Budapest Convention on Cybercrime** (ETS 185). That protocol aims to lay down provisions for a more effective and simplified MLA regime as well as provisions allowing for direct cooperation with service providers in other jurisdictions. It shall be equipped with a framework of strong safeguards for existing practices as regards cross-border access to data and data protection requirements. The preparatory work on the protocol started in September 2017. The drafting group agreed, inter alia, to engage in close consultation with civil society, data protection organisations and industry in the drafting process which was expected to be finalised by December 2019, and also to **closely coordinate that work with the preparation of relevant legal instruments by the EU**[6].

5. As underlined in the 2016 Council conclusions, service providers play a fundamental role in matters related to cross-border access to e-evidence. Improving cooperation with them is therefore essential. Since the main global players are based in the US and are subject to US law, legislative and judicial developments occurring there also impact the process ongoing within the EU.

6. The case of **US vs. Microsoft Corporation** pending before the US Supreme Court raises the question of whether, under the Stored Communications Act of 1986, US law enforcement authorities can require a US-based service provider, on the basis of a judicial warrant, to produce the content of an email account stored on a server located overseas. The decision is expected by June 2018. The Commission on behalf of the EU submitted an amicus brief in support of neither party on the basis of elements provided during the consultation process in the Council.

---

**6** https://rm.coe.int/t-cy-pd-pubsummary/168076316e

7. However, this case could become moot, if a new bill introduced in Congress on 6 February (the **Clarifying Lawful Overseas Use of Data (CLOUD) Act)** were to become law. The bill has industry support[7], as well as of the US Department of Justice, but is criticised by certain privacy NGOs[8]. The CLOUD Act would amend the Stored Communications Act of 1986, by stipulating that US service providers are obliged to comply with US orders to disclose content data regardless of where such data is stored. In addition, it sets the requirements under which the US Administration may conclude executive agreements, which would allow US service providers to deliver content data to a partner foreign government (as well as intercept wire communications), without the need for an MLA request . In addition, through a "comity clause", the CLOUD Act enables service providers to request a US court to quash or modify an order issued for data stored overseas if the data relates to a non-US person and if complying with the warrant would cause them to violate the laws of a partner country with whom the US has entered into an executive agreement that provides similar possibilities to service providers under their laws (i.e. to invoke a conflict of laws and to notify their government of the order). The court could quash the order if, by assessing the interests at stake, it would consider that this would be in the interest of justice.

8. This topic is likely to be raised further on during the discussions at the EU-US Ministerial Meeting, scheduled for 22-23 May in Sofia.

9. The developments briefly outlined above represent just a few examples demonstrating the complex and **dynamic nature** of issue at hand and also the **urgent need to take action at EU level.** The process ongoing within the EU cannot and should not be led in isolation from those international developments but the speed of these developments can substantially change the setting in which the EU action was prepared so far and slow down the process by having to consider an evolving regulatory situation.

---

7 For example, Apple, Oath, Google, Facebook and Microsoft support letter (https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf).

8 For example, Access Now, the Electronic Frontier Foundation, the Center for Democracy & Technology.

10. Against this background,

Commission is invited to update delegations on the current state of play of this file, taking into account the issues as described above, and to outline the next steps together, if possible, with their respective timeline;

delegations are invited to exchange views on the subject of cross-border access to e-evidence, in particular on the international developments and their approach to them, and other elements they wish to bring forward such as national developments, regulatory or other, emerging needs or new challenges stemming from on-going investigations and criminal proceedings, and their ideas for the way ahead.