Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward

I. Context

In the April 2015 Communication on a European Agenda on Security,[1] the Commission committed to reviewing obstacles to criminal investigations on cybercrime, notably on issues of access to electronic evidence, and announced an initiative on access to electronic evidence in its 2017 Work Programme.[2] In its June 2016 Conclusions[3], the Justice and Home Affairs Council highlighted practical and legal obstacles to criminal investigations in a cross-border context. For most forms of crimes, in particular cybercrimes as witnessed recently, electronic evidence – such as account subscriber information, traffic or metadata, or content data – can provide significant leads for investigators, often the only ones. The electronic evidence connected to these crimes is often cross-jurisdictional, for example because the data is stored outside the investigating country or by providers of electronic communications services and platforms[4] – whose main seat is located outside the investigating country, resulting in investigating authorities not being able to use domestic investigative tools. In this context, and in an evolving and volatile cyber threat environment, the Council asked the Commission to find ways to secure and obtain electronic evidence more quickly and effectively.

The current legal framework for cross-border access to evidence consists of bilateral and multi-lateral mutual legal assistance (MLA) instruments, replaced as of 22 May 2017 within the EU by the European Investigation Order (EIO);[5] the Budapest Convention;[6] and national regimes of Member States and third countries. Cross-border access to electronic evidence may be obtained in three ways:

- through formal cooperation channels between the relevant authorities of two countries, usually through MLA/EIO (where applicable), or police-to-police cooperation;
- through direct cooperation between law enforcement authorities of one country and service providers whose main seat is in another country, either on a voluntary or mandatory basis; notably service providers established in the United States (U.S.) and Ireland reply directly to requests from foreign law enforcement authorities on a voluntary basis, as far as the requests concern non-content data;

[1] COM(2015) 185 final.
[2] COM(2016) 710 final.
[3] Conclusions of the Council of the European Union on improving criminal justice in cyberspace, ST 9579/16.
[4] The exact definition of electronic communication services and platforms will be further developed during the preparatory work, aiming at including all type of data that could be relevant for criminal investigations. For a description of platforms, please see the Commission Staff working document on online platforms and the Digital Single Market, COM(2016) 288.
[5] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, p.1. The EIO will bring significant improvements compared to MLA proceedings, with the caveat that Ireland and Denmark are not participating in it. To ensure the full effectiveness of these improvements and of those to be achieved by the practical measures described hereafter, Member States need to transpose and implement the EIO Directive in a timely manner. By 19 May 2017, only DE, RO, SI and FR had communicated national transposition measures.
[6] The Convention on Cybercrime of the Council of Europe (CETS No 185).

- through direct access from a computer, as allowed by a number of Member States' national laws.

The current legal frameworks reflecting traditional concepts of territoriality are challenged by the cross-jurisdictional nature of electronic services and data flows. A number of Member States and third countries have developed or are developing national solutions that might result in conflicting obligations and fragmentation and create legal uncertainty for both authorities and service providers.[7] Consequently, the Council identified all three current channels as being in need of improvement.

In response, the Commission launched an expert process with a wide range of stakeholders, including Member States' Ministries, judiciary and law enforcement, industry, civil society, academia, EU agencies and others. This paper suggests ways forward on the basis of findings of the expert process.

II. Practical measures to improve cross-border access to electronic evidence

The experts have identified a number of practical measures that can improve cooperation among law enforcement and judicial authorities and with service providers within the current legal framework.

1. Improving cooperation among judicial authorities

Within the EU

To enhance judicial cooperation within the EU in the framework of the EIO, the following practical measures are being implemented:

- Creation of an electronic user-friendly version of the EIO form annexed to the EIO Directive, to facilitate completion and translation of this form, including guidance that allows practitioners to fill it in without having followed dedicated training;[8] this work has been carried out with a dedicated expert group of representatives of Eurojust, the European Judicial Network in criminal matters and the European Judicial Cybercrime Network, and a pilot version is ready to be launched. This electronic form will be made available on the EJN website, and it will later be incorporated into the platform mentioned below;
- Making available a platform with a secure communication channel for digital exchanges of EIOs for electronic evidence and replies between EU judicial authorities[9]. Work on this platform is ongoing based on the technical architecture agreed with the Member States, which include comprehensive security requirements[10].

[7] Please see the problem definition contained in the technical report and in the Commission's December 2016 Progress Report to the Council of the European Union, ST 15072/1/16.
[8] This work does not imply a modification of the form, but e.g. pre-defined scroll-down menus to select from.
[9] A later extension of this cooperation platform to US authorities could be considered, if Member States and the US would consider this useful. The possibility to expand the cooperation platform to include secure communication channels with private entities could also be examined at a later stage.
[10] The experts considered that the exchange platform should use the e-CODEX system. Whether e-Codex can be used needs to be further assessed, without prejudice to the impact assessment that the Commission is undertaking on the sustainable maintenance of the e-CODEX system as such.

With the US

Looking beyond the EU, the Commission is pursuing the following practical measures to improve cooperation between Member States' authorities and U.S. authorities:

- Organising regular technical dialogues between the Commission and the U.S. Department of Justice to continue to improve the treatment of MLA requests for electronic evidence;
- Facilitating regular dialogues between the Commission, the EU Delegation to the U.S. and liaison magistrates of Member States in the U.S. to discuss issues affecting the MLA process;
- Providing opportunities for exchange of best practice and training for EU practitioners on relevant U.S. law and procedures, notably on the U.S. legal standard of probable cause. The Commission is making available € 500.000 to fund the creation of training materials and the organisation of courses, meetings and conferences;[11]
- Establishing an online platform to provide information on applicable rules and procedures to facilitate the creation of requests.[12]

2. Improving cooperation with Service Providers

Direct cooperation between Member States' authorities and service providers based in another jurisdiction on a voluntary basis has de facto become the main channel for law enforcement and judicial authorities to obtain non-content data. While U.S.-based service providers are able to provide non-content data to foreign law enforcement under U.S. law, in the EU, only service providers based in Ireland are able to do the same. These two countries account for a large proportion of the total volume of requests. To improve direct cooperation with service providers and thus facilitate access to evidence, the experts identified the following set of practical measures that should be taken:

- Establishing Single Points of Contact within Member States' authorities that can ensure the quality of outgoing requests and build relationships of confidence with providers;[13]
- Establishing Single Points of Contact on the service providers' side that can serve to clarify provider policies;[14]
- Streamlining service providers' policies to reduce the heterogeneity of approaches, notably regarding procedures and conditions for granting access to the requested data;
- Standardisation and reduction of forms used in Member States to facilitate the creation of quality request. A key element is that service providers have full confidence when it comes to the identification of authorities and the forms used;
- Developing training programmes and exchange of best practice for EU law enforcement and judicial authorities for cooperation with U.S.-based providers. The Commission is making available € 500.000 for this purpose;[11]
- Establishing an online information and support portal at EU level to provide support to online investigations, including information on applicable rules and procedures.[15]

[11] On 4 May 2017, the Commission launched a call for proposals with a total budget of €1mln for improving cooperation between judicial authorities of EU Member States and both U.S. judicial authorities and U.S.-based service providers (€ 500.000 each) under the Partnership Instrument Annual Action Programme 2016 (EuropeAid/155907/DH/ ACT/Multi). More information is available at http://ec.europa.eu/europeaid/about-funding_en.

[12] This portal is distinct from the cooperation platform for EU judicial authorities mentioned in section II.1.

[13] Such SPOCs are already in place in a number of Member States, including BE, FI, FR, UK.

[14] A number of providers have established dedicated law enforcement portals to provide guidance, including Apple, Facebook, Google and Microsoft.

It should be noted that the effectiveness of these practical measures also depends on a number of factors, notably the (continuing) willingness of service providers to cooperate. As the voluntary cooperation with service providers based in the U.S. and Ireland is limited to non-content data, any improvement would not extend to content data (which can currently only be accessed through MLA), nor to non-content data controlled by service providers based elsewhere.

III. Legislative measures to improve cross-border access to electronic evidence

The proposed practical solutions can only partly address the identified problems, as they cannot provide solutions for fragmented legal frameworks among Member States. This fragmentation has been identified as a major challenge by service providers seeking to comply with requests based on different national laws. The practical solutions would also not address the need for increased legal certainty, transparency and accountability in direct cross-border cooperation between authorities and service providers, which was highlighted as a key issue by all stakeholders in the expert process. Both mutual recognition and MLA procedures can and should be streamlined and made more efficient. However, countries hosting major service providers or data centres on their territory already face challenges in coping with an ever-increasing number of requests for electronic evidence, which also explains why direct cooperation takes place in such countries (the U.S. and Ireland). Therefore, any legislative solutions to improve the current framework should address these issues. Such legislative solutions would be subject to an impact assessment, which would include their legal feasibility under the relevant provisions of the TFEU, notably Article 82.

1. Legislative solution: production requests/orders

One of the solutions identified by experts is an EU legal framework for investigative measures addressed to a service provider enabling authorities to request ("production request") or compel ("production order") a service provider in another Member State to disclose information about a user.

Production requests or orders would be used when a third party (not the suspect) is in possession of the data sought. Such an EU legal framework could allow law enforcement and judicial authorities to address production requests/orders directly to service providers whose main seat is in another Member State, and allow or compel service providers with a presence in the EU to respond to such requests/orders, without going through a law enforcement/judicial intermediary in the other Member State.[16] Such a production request/order could take several forms: one possibility would be to establish a legal basis for authorities to act and service providers to respond voluntarily; on the other end of the scale would be a mandatory production order with a sanctions regime, e.g. in the form of fines, as a means to enforce it. An EU instrument could define common conditions and minimum safeguards for such measures, as well as mitigating measures such as notification requirements.

Creating such an EU framework would provide legal certainty for cross-border requests/orders and reduce both the level of complexity and fragmentation for service providers and the conflicts of laws within the EU. It would create a new dimension in cooperation in criminal matters among Member States.

[15] Europol's SIRIUS portal already responds to this goal.
[16] In all cases, the material jurisdiction over the case would be established according to national law.

A possible option to facilitate the processing and the enforcement of production requests/orders by a judicial and/or law enforcement authority of an EU Member State, electronic communication services and platforms providers based outside the EU could be required to appoint a legal representative in an EU Member State according to criteria to be defined. This legal representative could serve as a recipient for production requests/orders directed to that company (from any Member State authority) and also for enforcement measures such as fines. The production request's/order's mechanism as described above would then apply, meaning that a coherent legal framework would be applied by law enforcement and judicial authorities to all relevant service providers, whether they have headquarters in or outside the Union. The applicable legal basis , modalities and feasibility of these requirements would have to be carefully considered beforehand to ensure full compliance with EU international commitments.

Additional issues arise when the data to which access is sought is held outside the EU, as the production request/order will then be directed to data that is subject to the jurisdiction of a third country. The ensuing territoriality and reciprocity concerns are further discussed below.

2. Legislative solution to facilitate direct access

In some situations the location of data, infrastructure or a service provider cannot be established ("loss of knowledge of location situations") or there is a risk of losing data. In such cases, a number of Member States already today provide for possibilities to access and in some cases copy the data directly from a computer system. The experts suggest that at EU level common conditions and minimum safeguards for such direct access in potential cross-border situations could be defined, as well as mitigating measures such as notifications to other possibly affected countries. Such common conditions and safeguards would aim to reinforce mutual trust and loyal cooperation between the Member States while preserving national measures where they exist. Alternatively, this could also be limited to providing a common framework for notification of another (Member) State affected, while not touching the domestic regime for direct access.

3. International Agreements

The possible legislative measures described above could be complemented by EU level bilateral agreements with key partner countries (such as the U.S., which receives the highest volume of requests[17]) and/or through expanding multilateral treaties, in particular the Budapest Convention[18]. Such measures could concern both cooperation with service providers and direct access with the aim to create more legal certainty and embed the necessary safeguards.

4. Further considerations for legislative solutions

When contemplating measures to facilitate access to cross-border electronic evidence, questions of territorial jurisdiction, the protection of individuals' rights, in particular in criminal proceedings, as well as fundamental rights such as data protection and privacy, will have to be assessed and taken into consideration.

[17] An agreement with the U.S. could in particular allow direct requests to service providers for content data that can currently not be disclosed by U.S. service providers under the voluntary cooperation regime in place. Such an agreement would fall within the scope of application of, and would thus have to comply with, the EU-US Umbrella Agreement.

[18] At its November 2016 meeting, the Convention Committee (T-CY) of the Council of Europe Budapest Convention on Cybercrime, "agree[d] in principle on the need for an Additional Protocol", T-CY (2016)32.

As regards the protection of individuals' rights, the right to fair trial is of particular importance when it comes to criminal proceedings. Any legislative initiative should respect this principle and include safeguards to protect the rights of the persons affected, including the rights of the defence, the right to an effective remedy as well as other procedural rights. However, given that the possible measures could require individuals to challenge measures in a court of a Member State other than their own, the possibilities of effective judicial redress for persons who may be affected by such measures, including operators and other persons not involved in the criminal proceedings, would also have to be addressed.

Another important aspect is the need to guarantee the fundamental rights to data protection and privacy. Subscriber information, traffic data, metadata, and content data are personal data, and are thus covered by the safeguards under the EU data protection acquis.[19] In the context of the possible measures, the type of data – as well as other factors such as for instance the volume of data to be accessed or the type of investigative measure – may be relevant for assessing the intensity of the interference to the fundamental right to data protection, and therefore for determining whether such interference respects the principle of proportionality.

Owing to the fact that the concept of territoriality is still based largely on the place where data is stored, any cross-border access to electronic evidence that is not based on cooperation between authorities may raise issues in terms of territoriality. This applies both within the EU and where data is stored in a third (non-EU) country. Already in the EU, Member States do not always agree on when a relevant "cross-border element" affects the territory of another Member State. Common EU criteria could address this issue. These criteria can provide conditions to be fulfilled for certain investigative measures, and may trigger further obligations such as the notification of the other state concerned. The experts have expressed the view that there is a need to move away from data storage location as the (only) relevant criterion.[20] Instead, a number of factors should be considered, including the place of main establishment of the data controller and/or the place of residence of the person targeted by the measure.

In this context, another important aspect to consider is possible reciprocal responses by third countries, aiming to reciprocally access data stored in Europe. This would be problematic if the third country does not have fundamental rights safeguards in place that can be considered comparable to ours, including in the field of data protection. At the same time, it should be stressed that a number of third countries most likely would not need to rely on reciprocal responses, as they have already put in place solutions to ensure access to data, such as data localisation obligations or a wider set of investigative measures. In fact, at a time when some third countries might be tempted to adopt unilateral approaches for obtaining electronic evidence (e.g. data localisation obligations or a more expansive set of investigative measures), creating a framework for access to electronic evidence that builds on the robust protections already provided for under EU law and including specific safeguards could also set a positive example.

IV. Suggested way forward

In order to improve cross-border access to electronic evidence, the Commission suggests pursuing the implementation of all practical measures outlined above.

[19] Personal data is any information related to an identified or identifiable natural person, Article 4(1) GDPR.

[20] Data storage normally takes place outside the control of the state on whose territory data is stored. If data storage were to be retained as a relevant element, possible policy responses would forcibly have to include data localisation requirements.

To build on these practical measures and to create a more robust legal framework, the Commission services seek the views of the Council regarding the feasibility and necessity of legislative measures set out above, and on taking forward preparatory work with a view to a possible concrete initiative.