Council of the European Union

Brussels, 7 December 2016
(OR. en)

15072/1/16
REV 1

JAI 1037
CYBER 143
COPEN 369
DROIPEN 206
JAIEX 103
EJUSTICE 210
ENFOPOL 459

COVER NOTE

From:	Commission Services
To:	Delegations
No. prev. doc.:	14711/16, 10007/16
Subject:	Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace

Delegations will find attached a non-paper from the Commission Services: Progress report following the Conclusions of the Council of the European Union on improving criminal justice in cyberspace.

NON-PAPER:

PROGRESS REPORT FOLLOWING THE CONCLUSIONS OF THE COUNCIL OF THE EUROPEAN UNION ON IMPROVING CRIMINAL JUSTICE IN CYBERSPACE

1. INTRODUCTION

Crime leaves digital traces that can serve as evidence in court proceedings; often it will be the only lead law enforcement authorities and prosecutors can collect. Therefore, effective mechanisms to obtain digital evidence are of the essence. However, present-day solutions too often prove unsatisfactory, bringing investigations to a halt. Moreover, there have been a number of court cases raising important questions of jurisdiction over data stored abroad by a service provider whose main seat is within the requesting state, including notably the Microsoft Ireland case in the U.S.[1]. Other examples are the Yahoo![2] and Skype[3] decisions in Belgium covering the use of domestic production orders for companies providing a service on Belgian territory, or the Gmail case in Germany on whether email is a telecommunications service.[4]

In the April 2015 Communication on a European Agenda on Security,[5] the Commission committed to addressing these challenges for investigations into cyber-enabled crimes. This was confirmed in the 20 April 2016 Communication on delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union.[6] In the Communication, the Commission undertook to propose solutions by summer 2017, including legislation if required, to address the problems of obtaining digital evidence in relation to criminal investigations.

In its Conclusions on improving criminal justice in cyberspace, adopted on 9 June 2016 (hereafter: the Conclusions),[7] the Council supported the Commission´s commitment and called on the Commission to take concrete actions based on a common EU approach to improve cooperation with service providers, make mutual legal assistance more efficient and to propose solutions to the problems of determining and enforcing jurisdiction in cyberspace.

The Council requested the Commission to report on intermediate results by December 2016 and to present deliverables by June 2017. The present report details the Commission's activities between July and November 2016 and describes the problems identified.[8]

---

1 U.S. Court of Appeals for the Second Circuit, Microsoft v. United States, No. 14-2985 (2d Cir. 2016) of 14 July 2016; the Department of Justice has requested review of the case.

2 Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N of 1 December 2015.

3 Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12 of 27 October 2016; it has been reported that Skype has appealed the decision.

4 VG Köln, Az. 21 K 450/15 of 11 November 2015; currently under appeal.

5 COM(2015) 185 final

6 COM(2016) 230 final

7 Conclusions of the Council of the European Union on improving criminal justice in cyberspace, 9 June 2016.

8 Although data retention and encryption are part to the issues raised by access to e-evidence these issues belong to a different context and are therefore not included in the report.

The three building blocks of the Conclusions, namely direct cooperation with service providers, mutual legal assistance and enforcement of jurisdiction in cyberspace, were the starting reflection axes of Commission services.

The Commission services launched a comprehensive expert consultation process in July 2016 which is expected to run until June 2017, including a detailed questionnaire.

The consultation is designed to allow for a gradual development of the possible options and scenarios and will gradually increase the number of stakeholders involved. The Council and the European Parliament will be kept informed and invited throughout the process.

1.1. Expert process

To define and scope the problems, to map different initiatives, to draw up possible options and identify first practical solutions, the Commission services organised various bilateral meetings: with Member States, including the Presidency, with other stakeholders, including the Council of Europe, Interpol, UNODC, the European Judicial Network but also with a number of private sector service providers and civil society organisations.

A series of targeted meetings with specific experts from various backgrounds were also organised:

- On 12 July 2016 an experts' meeting with academics and practitioners from Member States took place covering the relationship between different channels for obtaining cross-border access to electronic evidence, including direct cooperation and Mutual Legal Assistance, as well as the concepts of establishing investigative jurisdiction and enforcing jurisdiction.
- On 15 September 2016, in conjunction with the EU Internet Forum, the Commission services held a workshop with service providers (including Microsoft Google, Apple, Twitter and Facebook representatives) and members and representatives of industry associations (CCIA, BSA and DIGITALEUROPE) that issued a supporting statement[9], with the objective to compare assessments of the current status quo and exchange views
- On 4 October 2016 an experts' meeting with Member State practitioners, European Judicial Network (EJN) and Eurojust representatives discusses the use of Mutual Legal Assistance within the Union, notably the possible use of the European Investigation Order (EIO) for cross-border access to electronic evidence and in particular its annex A with regard to its suitability for requesting access to digital evidence, as well as the possible requirements for an IT portal to exchange requests.
- On 9 November 2016, an expert meeting with representatives of Member States, the EJN, Eurojust and the Council secretariat, and technical experts working on e-codex MLA, Interpol and Evidence projects discussed the way forward towards "a secure online portal" for requests and responses concerning e-evidence.

[9] Joint statement of The Computer & Communications Industry Association (CCIA Europe), BSA │The Software Alliance, and DIGITALEUROPE of 10 June 2016 on the 9 June 2016 Conclusions of the Council of the European Union on improving criminal justice in cyberspace.

The Commission also presented its work at events organised by the Internet & Jurisdiction project in July and November 2016; at a workshop organised by DIGITALEUROPE and a panel discussion on cybercrime organised by the Permanent Representation of Hessen in September 2016; at the European Chiefs of Cybercrime Units (EUCTF) meeting in October 2016; and at a workshop organised by Public Knowledge on "Challenges of Cross-Border Data", the Forum Europe 4th Annual Conference on Cybersecurity, a CEPS seminar on "EUnited against crime: improving criminal justice in European Union cyberspace" and several workshops of the Council of Europe Octopus conference in November 2016.

The European Judicial Network meeting of 21-23 November 2016 allowed reflection on the form to be used. The European Judicial Cybercrime Network, a network bringing together specialised prosecutors from the 28 Member States to exchange expertise, best practices, legal analysis and practical experiences on cybercrime issues, was launched on 24 November 2016 as foreseen by the 9 June 2016 Council Conclusions on the European Judicial Cybercrime Network. In the coming weeks the network will establish its work program for 2017-2018.

A number of other actors have also made finding solutions to these and related problems a key priority and are actively working on them in parallel processes. This enabled the Commission services to build on input and previous reflections from a variety of sources, including the Council of Europe (Cloud Evidence Group), Interpol, bilateral and unilateral efforts at Member States' and third States' level, academic research and many conferences. The Commission services have sought to ensure close coordination of their work with efforts under way elsewhere and have also benefited from the expertise of Europol and Eurojust.

The reflection process also drew on results of previous work in the EU, notably on the March 2016 Amsterdam conference on Crossing Borders: Jurisdiction in Cyberspace organised by the Netherlands Presidency of the Council of the EU, and on the first results of the Council of the European Union Working Party on General Matters including Evaluation (GENVAL) 7th Round of Mutual Evaluations on Cybercrime.

1.2. Questionnaire

The Commission services circulated a questionnaire on cross-border access to electronic evidence amongst Member States, which was developed taking into account previous and ongoing activities, including the GENVAL evaluation, and sought to complete the picture. The questionnaire was launched on 29 July 2016 and closed in October 2016. The detailed replies received from 24 Member States (all except BG, LU, MT and PL) provided valuable additional information which is reflected below. The national replies were coordinated at national level amongst different responsible ministries, the judiciary and law enforcement authorities, providing a comprehensive overview of the current state of play within the Member States.

The questionnaire focusses on current practices in the Member States concerning 1) **direct cooperation** between law enforcement authorities and private sector service providers, 2) **mutual legal assistance** or mutual recognition procedures and 3) enforcement of **jurisdiction in cyberspace**, namely other measures that law enforcement authorities could use to obtain e-evidence in cases when it is not clear they would operate within their own jurisdiction.

The replies revealed that there is **no common approach** to obtain cross-border access to digital evidence, for which each Member State has developed its own domestic practice. There is a large variety of approaches adopted by the Member States and their law enforcement and judicial authorities as well as by the service providers. This diversity, which seems mainly due to the lack of a legal framework and of a common approach on how to access e-evidence and deal with requests to share information, creates legal uncertainty for all the stakeholders involved and represents an obstacle to joint and cross border investigations.

1.2.1. Direct cooperation, in particular when the service provider is outside the domestic jurisdiction

- EU Member States and their judicial and law enforcement authorities have taken diverging approaches as regards the use of the connecting factors for the exercise of an investigatory measure allowing for access to e-evidence. There are different ways of determining whether a provider is to be considered domestic or foreign and the criteria to distinguish between domestic and foreign service providers vary significantly among the Member States, ranging from the "main seat of the service provider" (16 Member States) and "the place where services are offered" (6 Member States) to "the place where data is stored" (6 Member States) and a combination of alternatives.
- Moreover, while 14 Member States consider direct requests sent from national authorities directly to a service provider in another country as voluntary for the provider to comply with, 7 Member States consider these requests as mandatory. Even when this mechanism is considered mandatory, it is very difficult to assess whether the Member States can actually enforce it, also due to the lack of a specific legal framework for these requests (20 Member States apply to these cases the same framework as for domestic requests) or agreement with foreign service providers (only 8 Member States have such agreements).
- The majority of national legislations either do not cover or explicitly prohibit that service providers established in the Member State respond to direct requests from law enforcement authorities from another EU Member State or third country[10].
- The definition of types of data (subscriber, traffic and content data) varies significantly among Member States, while specific categories of data exist in several countries. Data requested from service providers are generally subscriber (21 Member States) and traffic data (18 Member States), while in a few Member States (9) it is also possible to request content data and "other data" (4 Member States).
- Practices also diverge as regards the procedures for making the direct requests, i.e. the authority which can initiate the process (generally the police, followed by the prosecutor and the judge), the modality for launching a request or transmitting e-evidence (normally via email or web portal, but in some other cases with paper or fax or via all the possible means). The only common feature is the lack of a central repository in the Member States.
- There is no common approach on how the service providers react to requests from foreign law enforcement authorities and it appears they respond differently depending on which country requests come from, with a minimum responding time of a few minutes in certain countries to a maximum of 1 month in others.

[10] As regards third countries, the General Data Protection Regulation (Regulation (EU) 2016/679) and the Directive on data protection in the police and criminal justice field (Directive (EU) 2016/681) applicable from May 2018 set certain requirements on transfers of personal data in this context.

- Admissibility in Court of e-evidence gathered outside the MLA mechanism does not generally constitute a problem for the majority of Member States, with the exception of a few Member States where this is not allowed by domestic laws or it is subject to stringent conditions, showing the lack of a common view on the principle of voluntary disclosure without an MLA among Member States.

1.2.2. Mutual Legal Assistance (MLA) with third countries

- As regards cooperation with countries outside the European Union, Mutual Legal Assistance (MLA) is in this area mainly based on international law, notably the Council of Europe Budapest Convention on Cybercrime. Besides that, there are agreements concluded by the EU (notably, the Agreement on MLA between the EU and the U.S.) and several bilateral agreements, which most Member States have concluded with the US, followed by Canada and China.
- The systematic use of MLA for all types of access requests for electronic evidence is increasingly viewed as problematic as the requests take too long to be processed (a minimum of 1 month to a maximum of 18 months), there are no fixed deadlines for responding, and the mechanism is complex and diverges from country to country (i.e. in most of the countries the formal procedure for issuing an MLA is initiated by prosecutor, followed by judge, law enforcement, diplomatic channel or central authorities).
- When it comes to cooperation with the U.S. in particular, challenges identified concern the use of MLA procedures for access to information where under U.S. law no MLA request is required, such as for subscriber or traffic data. MLA requests for such information significantly increase the overall volume of requests and contribute to slowing down the system. The use of MLA for such requests can be attributed to various reasons, including (1) where the issuing of a direct request is not permitted under the law of the issuing country; (2) where enforceability of the request is desired; and (3) a lack of awareness of the issuing authority about alternative channels.
- The admissibility of MLA requests is subject to the receiving countries' legal system, which may result in a refusal of the MLA request (most Member States indicated as ground for refusal the difficulty to establish probable cause, followed by the lack of dual criminality, data not available due to deletion, incomplete or inadequate requests).
- MLA is often used to obtain access to content data (22 Member States), but it is also used to obtain other types of information, including subscriber and traffic data. "Top" third countries to which most Member States send the requests are the US and Canada.
- Although MLA requests are made following formal channels, it is difficult to keep track of both requests and responses to third countries with the effect that most Member States do not have available statistics for e-evidence.
- The means of transmission are generally inadequate as most of the Member States make use of letter, fax or email, with very few countries using secure channels.

1.2.3. Enforcement of jurisdiction in cyberspace

- EU Member States have taken different approaches in allowing their law enforcement and judicial authorities to use alternative mechanisms to obtain cross-border access to electronic evidence in the specific circumstances indicated below.

- Indeed, there are cases where it is impossible to determine a service provider responsible for the processing or storage of data. In these cases, law enforcement authorities make use of different techniques across the EU, such as, according to the replies, "police-to police cooperation", "agency to agency cooperation", "international legal assistance", "obtaining of consent of the person", "search and seizure techniques". Most of the EU countries, however, indicated the impossibility for law enforcement authorities to access e-evidence under these complex circumstances.
- In some Member States, law enforcement authorities make use of investigative techniques to access e-evidence also when the location of e-evidence is unclear or impossible to establish. Tools used across the EU range from "remote access" and "search and seizure" to "multiple MLA requests" and "instruments of international cooperation". On the other hand, there are still several countries (8 Member States) where the access to e-evidence under these circumstances is not possible or provided for by law.
- Evidence gathered through police to police cooperation is generally admissible before the court, however, there are several EU countries in which admissibility is subject to stringent conditions or to a MLA or it is not foreseen by law and rather considered as "intelligence".

2. PROBLEMS IDENTIFIED

The following sections detail the initial problem definition for the three areas on the basis of information gathered thus far. It will provide a basis for further discussion and refinement in the coming months.

2.1. Cooperation with service providers

For direct cooperation, the focus of input from stakeholders was on cooperation with U.S.-based service providers as those appear to be most relevant in practice for two reasons: 1) They hold a large proportion of relevant data; 2) U.S. law allows for direct cooperation. More specifically, section 2701(2) of the Electronic Communications and Privacy Act 1986 (ECPA) explicitly allows U.S.-based service providers (who represent by far the majority of receivers of data disclosure requests) to cooperate directly with European law enforcement authorities concerning non-content data. This cooperation is voluntary from the standpoint of U.S. law. Thus, providers have created their own policies or decide on a case-by-case basis on whether and how to cooperate.

The below outline seeks to reflect the main concerns raised by stakeholders from their various perspectives. It necessarily abstracts from companies' individual policies and procedures and may therefore not apply to all service providers and situations in an identical manner.[11]

[11] See for instance, Council of Europe Budapest Convention on Cybercrime Convention Committee (T-CY), Criminal justice access to data in the cloud: Cooperation with "foreign" service providers, T-CY (2016)2, provisional document of 3 May 2016.

While there are general concerns such as transparency of the process (see 3.1.1), reliability of the stakeholders (3.1.2) and their accountability (3.1.3), the involved parties also face concrete and practical issues like how to identify and contact the relevant service provider (3.1.4), or, on the provider's side, how to assess the authenticity and legitimacy of a request (3.1.5). Last but not least, the current practice reveals a large variety regarding the handling of requests for disclosing electronic evidence with no equal treatment across Member States (3.1.6), and this diversity also extends to the admissibility of evidence in court (3.1.7).

2.1.1. Transparency

A lack of transparency is cited as an issue from several perspectives:

Service providers have data protection obligations and wish to make it clear to the public that they take these obligations seriously, disclosing data only on the basis of a valid and legal request and notifying users where possible. However, sharing information about requests received may compromise an investigation. Service providers have therefore started to publish regular transparency reports based on aggregated data to prevent being seen as insufficiently transparent about protecting and disclosing customer information.

One of the major complaints from *law enforcement authorities* concerns the lack of transparency on the providers' side in relation to why a specific request is granted or refused and in which time frame. Investigating authorities often do not understand which arguments and procedures determine the final decision of the requested service provider.

User notification, as a tool for transparency, also creates its own challenges in cross-border situations for all parties involved, as national laws and company policies foresee different modalities and exceptions for user notification. In some Member States, it is obligatory for the investigating authority to provide notice to the user of an investigative act; in others, it is prohibited. The rules on when notice has to take place also vary widely or are entirely absent. This can lead to situations where Member States' authorities request data from a U.S. provider without realising that the provider will notify the user concerned unless a specific request to refrain from immediate notice is made and granted; this in turn may compromise an investigation under way.

2.1.2. Reliability

The process, regulated only through individual company policy on the provider side, is not predictable and thus not reliable for either side, service providers and law enforcement authorities. Data availability and service provider requirements and conditions for providing that data vary widely, as does the quality of law enforcement requests.

Service providers complain about the wide variety of request formats and about requests sent in a way that prevent authentication, e.g. if no secure channel of communication is used or the request is sent to a general info or press mailbox. Where forms are made available, they may be poorly filled out, sometimes due to language issues. Issuing authorities sometimes omit contact details, making follow-up questions difficult.

For *law enforcement authorities*, it can be unpredictable whether a request will be answered at all. As the cooperation takes place on a voluntary basis, providers are under no obligation to state reasons for refusal of disclosure or even to respond at all. Major service providers' approaches also differ with regard to the law enforcement agencies they will respond to, the supporting documentation they require, and the link to the investigating country that they demand. For example, while one provider requires that an underlying IP address resolve to the investigating country, another will provide data as long as the IP address does not resolve to the U.S. There are no binding deadlines for responses.

Even if law enforcement authorities are aware of certain procedures required by a company at a certain point of time, providers may change their policies at any time without notice.

2.1.3. Accountability

The problems of lacking accountability go hand in hand with those of transparency and reliability.

Service providers frequently have no insight into which crimes are being investigated as this may be confidential information. This makes it difficult for the providers to be accountable to their users. As data is provided without a legal obligation under U.S. law, service providers are also not accountable to law enforcement authorities for submitting no, incomplete or even false information. Requests are not enforceable under U.S. law; this would require going through mutual legal assistance instead.

Law enforcement authorities are held accountable through various processes including the need for prior authorisation by a judge and the possibility to refute admissibility of evidence gathered in violation of procedural rules in a later court proceeding. However, these processes are usually not designed to take account of this direct cooperation across borders and therefore are deemed unsatisfactory by some.

2.1.4. Difficulty to identify and contact the relevant service provider

Law enforcement authorities report problems in identifying which service provider can provide data on, e.g., an email account encountered during the investigation. Furthermore, while most service providers offer a special point of contact for an official request, these contact points may be at national level, set up for regions (like Europe), or even going directly to the seat of the company which may be anywhere in the world.

Even if the contact point has been clarified for a specific case, the actual contacting act can still be difficult: there is no common line among providers regarding the use of platforms, forms, required content of a request, language or communication channels. Law enforcement authorities have to tailor its approach to each individual company.

2.1.5. Assessment of authenticity and legitimacy of request

Most *service providers* assess whether the request complies with the domestic legal framework of the requesting authority. This extends to checking whether the requesting authority would have the power to request a certain type of data from a service provider at the domestic level, as a direct request to a foreign service provider, while permissible, is usually not explicitly provided for in national legislation. Taking this assessment seriously creates significant legal expenses for providers, especially since national provisions differ widely even among EU Member States.

Furthermore, in order to avoid civil and/or criminal liability for sharing data with unauthorized parties, the service providers have to ensure authenticity of the request. As it was mentioned before in the context of accountability, this can be difficult.

Member States' *law enforcement and judicial authorities* frequently view the assessment on compliance with national law as inappropriate. In their view, it should not be up to a private company to privately challenge a judicial assessment on whether conditions under national law for the disclosure of data are met. However, as there are no enforcement mechanisms attached to this form of cooperation, the service provider's assessment determines compliance.

2.1.6. No equal treatment across Member States

Law enforcement authorities from different Member States indicate that providers respond differently depending on where requests come from. This is confirmed by an analysis of transparency reports of some of the major service providers: the average percentage of disclosure of data following all requests sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2014 varied among EU Member States from 31 % (Poland) up to 78 % (the Netherlands) [12].

To illustrate the problem, the following sample numbers in relation to requests in 2014 following the transparency reports of the respective companies[13]:

Rate of disclosure of the requested data by a service provider to a Member State of the European Union:

Google / Youtube:	0 % (Hungary) - 83 % (Finland)
Facebook:	15 % (Austria) - 80 % (Croatia)
Apple:	29 % (France) - 90 % (Austria)

[12] Council of Europe Budapest Convention on Cybercrime Convention Committee (T-CY), Criminal justice access to data in the cloud: Cooperation with "foreign" service providers, T-CY (2016)2, provisional document of 3 May 2016.

[13] See for example transparency reports of: Apple (www.apple.com/privacy/transparency-reports/), Facebook (govtrequests.facebook.com/about/), Google (www.google.com/transparencyreport/), Microsoft (www.microsoft.com/about/csr/transparencyhub.

Rate of disclosure to a Member State following requests to different companies:

Austria:	27 % (Google / Youtube) - 90 % (Apple)
Germany:	38 % (Google / Youtube) – 79 % (Microsoft/Skype)
Hungary:	34 % (Facebook) - 83 % (Microsoft / Skype)
Slovakia:	8 % (Google / Youtube) – 81 % (Microsoft/Skype)

In addition, there are providers which do not reply to any requests at all.

2.1.7. Admissibility of evidence

Given that direct requests from law enforcement authorities in a EU Member State to service providers established elsewhere are not explicitly foreseen under most national laws of criminal procedure, there can be problems with the admissibility of evidence gathered through direct cooperation in a later criminal trial.

2.2. Mutual legal assistance and mutual recognition proceedings

Cross-border access to electronic evidence is often obtained on the basis of formal cooperation between the relevant authorities of two countries. The main mechanism for the formal cooperation between the competent authorities of different countries for obtaining cross-border access to electronic evidence is currently based on mutual legal assistance (MLA), both within the European Union and with third countries. Although MLA is most often used to obtain access to content information, MLA procedures are also used to obtain other types of information, including subscriber information and traffic information.

Within the European Union, the legal framework for the formal cooperation for obtaining cross-border access to electronic evidence is the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.[14] The Convention will be replaced by the Directive regarding the European Investigation Order (EIO) in criminal matters, which needs to be transposed by 22 May 2017 and is based on mutual recognition.[15] It involves direct communication between judicial authorities, provides for deadlines, standardised forms and a limited possibility to refuse execution of requests.

[14] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

[15] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

A key MLA Treaty for the formal cooperation for obtaining cross-border access to electronic evidence of European Union Member States' authorities is the Agreement on Mutual Legal Assistance between the European Union and the United States, which was subject to a review in 2016.[16] The Review Report identifies two main problems: EU Member States requests' are often not successful on the grounds of inadequacy, particularly because not meeting the US probable cause requirements; and, once accepted for execution, delays occur during the execution phase, the volume of requests to the US being particularly high. Because of the preponderance of the headquarters of service providers located in the U.S. and the data maintained there, the U.S. is the recipient of a large proportion of worldwide requests for electronic evidence. The Review Report contains recommendations concerning electronic evidence, notably that EU Member States may seek to obtain direct cooperation from ISPs in the USA in order to secure and obtain digital evidence more quickly and effectively, and that EU Member States and the U.S. will continue to consider what additional steps may be feasible to reduce the pressure of the volume of MLA requests to the U.S. for e-evidence and to enhance rapid preservation and production of data. Another recommendation is to raise the awareness of practitioners from EU Member States regarding the requirements of U.S. legislation in this area.

The use of mutual legal assistance proceedings is often considered as problematic for obtaining cross-border access to electronic evidence for criminal investigations. Stakeholders generally criticize that requests based on mutual legal assistance (1) take too long to be processed, (2) that processing takes up too many resources and is too complicated, and (3) that the process is insufficiently transparent.[17]

2.2.1. Length of time for processing

MLA is subject to formal procedures. These formal procedures ensure, amongst other things, that the right authorities are involved and that appropriate safeguards are taken into account. However, they also have the consequence that requests for mutual legal assistance require considerable time to be processed. Especially for electronic evidence, which is volatile in nature and can be transmitted, altered or deleted easily, lengthy mutual legal assistance proceedings are often considered as unsuitable.

2.2.2. Resource-intensive and complexity

Furthermore, the processing of formal requests for mutual legal assistance requires considerable resources, both on the side of the requesting and of the responding country. The requesting authority needs to draw up the formal request, which subsequently needs to be assessed and where relevant executed by the responding state. For requests for electronic evidence, mutual legal assistance proceedings are often considered as unnecessarily onerous.

---

[16] Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America.

[17] See for instance, Council of Europe Budapest Convention on Cybercrime Convention Committee (T-CY), T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, December 2014; Discussion paper on tackling cybercrime, Informal Meeting of the Justice and Home Affairs Ministers, Amsterdam 25-26 January 2016.

Likewise, issuing and responding to a mutual legal assistance request requires a significant amount of expertise. In order to follow the relevant formal procedures, specific expertise is necessary, including as regards the requesting and the receiving countries' legal system, e.g. on key elements like the admissibility of such requests. The complexity of procedures and requests requires experienced staff, which may not be available, which may result in incomplete or inadequate requests, the rectification of which requires additional steps to be followed.

2.2.3. Lack of transparency

Finally, requests for mutual legal assistance are often found to be insufficiently transparent. While requests are made following formal channels, it is often difficult to keep track of specific requests. In particular after sending a request, the authorities in the requesting country are often unaware of the state of play of a request.

2.2.4. European Investigation Order

Although the use of the European Investigation Order (EIO) will considerably improve the formal cooperation between the relevant authorities of Member States for obtaining cross-border access to electronic evidence, it has not been developed specifically with the objective to improve cross-border access to electronic evidence. Compared to direct cooperation with service providers, requests on the basis of mutual recognition are expected to be slower, more cumbersome and resource-intensive.

2.3. Enforcing jurisdiction in cyberspace

To complement the above possibilities, especially for cases where existing channels for obtaining cross-border access to electronic evidence are not sufficient or are not working properly, countries have developed other measures. These measures are partially grounded in the conviction, apparent throughout the expert consultations thus far, that a case presenting no links to the country/countries where the service provider has its main seat or where it has chosen to store the relevant data does not necessitate full involvement of that country's authorities. These mechanisms cover both the access to data held by a third party, as in the case of service providers (often referred to as the use of domestic production orders), and the access to data directly – without an intermediary – from a computer system within the territory of the investigating state.

2.3.1. The use of different connecting factors

Countries have different approaches to connecting factors, both when it comes to the use of production orders and to other investigative measures. As mentioned above, based on the results of the questionnaire, Member States refer to, inter alia, the place of the main establishment of a service provider, the place where a service provider has any another establishment, and the place where a service provider is offering services.[18]

[18] For reference, see for instance: Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N of 1 December 2015 and Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12 of 27 October 2016;

Other connecting factors that have been considered are the nationality of the suspect or the nationality of the victim that the electronic evidence pertains to.[19] A connecting factor for the exercise of an investigatory measure allowing for the access to electronic evidence that is often considered as significant is the location where electronic evidence is stored or processed, i.e. where the infrastructure that is used for the storage or processing of the electronic evidence is located.[20] Although there have been a few court decisions[21] about the obligations of service providers, enforceability remains a challenge unless the service provider is established in the relevant country.

At international level, reference can be made to the ongoing discussion amongst Parties to the Council of Europe Budapest Convention on Cybercrime on the application of Article 18(1)(b) of the Convention on the use of production orders for obtaining subscriber information. Discussions at the 14-15 November 2016 plenary meeting of the Convention Committee of the Budapest Convention on Cybercrime (T-CY) confirm that Parties to the Convention appear to have taken different approaches, and feel the need to consider the possibility of the negotiation of an additional protocol to the Convention that would provide for guidance on the use of approaches amongst Parties.[22]

The use of different approaches creates legal uncertainty for authorities issuing requests, as well as for service providers to which the requests are directed. Equally, as it is unclear to what extent a service provider is obliged to respond to a request based on different connecting factors, the legal uncertainty may also interfere with rights of the persons to which the requested evidence relates, including their right to privacy. Finally, the use of different approaches on connecting factors between different countries may be an obstacle to cross-border investigations.

2.3.2. The enforcement of investigatory measures

Although the use of the approaches outlined above to address cross-border situations may provide for a domestic legal title to direct a request for direct cooperation at a service provider, it does not necessarily provide for effective means for its enforcement.

Countries and their authorities rely on conventional enforcement mechanisms, including issuing fines and criminal penalties at national level where non-compliant service providers are located in another country. They also may rely on the country where the relevant service provider is established to obtain enforcement, using procedures based on MLA, which however contradicts the original intention behind the use of a domestic production order.

---

19 See for instance: Conings, C., "Locating criminal investigative measures in a virtual environment", 2014; Discussion paper on tackling cybercrime, Informal Meeting of the Justice and Home Affairs Ministers, Amsterdam 25-26 January 2016.

20 U.S. Court of Appeals for the Second Circuit, Microsoft v. United States, No. 14-2985 (2d Cir. 2016) of 14 July 2016; the Department of Justice has requested review of the case.

21 See for instance, Hof van Cassatie of Belgium, YAHOO! Inc., No. P.13.2082.N of 1 December 2015 and Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, No. ME20.F1.105151-12 of 27 October 2016;

22 Abridged meeting report of the 14-15 November 2016 Council of Europe T-CY 16th plenary meeting, T-CY (2016)32 of 15 November 2016.

2.3.3. The loss of location

It may not be feasible or possible for an authority to determine which service provider is responsible for the storage or processing of electronic evidence, or to determine the location of infrastructure used for the storage or processing of electronic evidence. Increasingly, criminals have the access and ability to make use of sophisticated techniques that allow hiding the location of infrastructure for the storage or processing of electronic evidence.[23]

Equally, the circumstances of a particular investigation may not allow determination of the responsible service provider, or the location of infrastructure for the storage or processing of electronic evidence, for instance in emergency situations or investigations where electronic evidence can only be secured within a limited timeframe.

Following the results of the questionnaire it appears that Member States have taken different approaches as regards the ability of law enforcement and judicial authorities to use mechanisms for obtaining cross-border access to electronic evidence under these circumstances.

Investigatory measures considered by countries are the interception of communications, or measures that allow for unmediated forms of access to electronic evidence by law enforcement authorities, e.g. by accessing an information system remotely. Member States' approaches are very heterogeneous. These different practices may result in legal uncertainty for authorities, service providers and data subjects, and may hamper joint and cross-border investigations.

Additionally, the development, and notably the use of investigative measures may be considered as having a certain effect beyond the borders of the country of a law enforcement or judicial authority. Although the impact of the development and use of investigative measures may be trivial depending on the circumstances of an investigations and type of investigative measure, the exercise of such a measure may easily be challenged by another affected state under current principles of international law, where the territorial sovereignty of nation states is considered as a key principle.

3. AVENUES FOR FURTHER EXPLORATION

The following sections provide an overview of ideas that have emerged thus far during the information gathering and expert process under way and that the Commission services, in consultation with stakeholders, will look into further in the coming months in line with the June 2016 Council conclusions.

[23] See for instance: Discussion paper on tackling cybercrime, Informal Meeting of the Justice and Home Affairs Ministers, Amsterdam 25-26 January 2016; the Europol Internet Organised Crime Threat Assessment (iOCTA) 2016, e.g. on Darknets and hidden services.

3.1. Practical improvements

The Council conclusions requested that the Commission identify ways to streamline the use of mutual recognition procedures. Practical improvements within the existing rules could be achieved by enabling swift exchange of digital evidence between competent authorities in the framework of the European Investigation Order and by identifying improvements for the cooperation between Member States' law enforcement agencies and service providers.

3.1.1. Improving the exchange between competent authorities

One of the deliverables referred to in the Council Conclusions is "a secure online portal" for requests and responses concerning e-evidence. At the experts' meetings of October and November 2016, practitioners expressed the wish to have a global/interconnected system, without multiplying the systems and forms that are already in use. The issue of the means of transmission of requests for e-evidence and of e-evidence itself among Member State authorities was further discussed at the experts' meeting of November 2016 on the basis of a discussion paper circulated beforehand describing the possible options and implications.

In summary, Member States indicated that any system design should be flexible enough to support different approaches in the Member States in terms of the authorities which should have access, and that any system must use proper authentication and authorisation measures to provide for the necessary security. The security level should be the same for requests and the responses thereto. Links with the case management systems of the Member States should not be considered initially. The communication of the requests and the responses thereto should take place through e-CODEX, with the relevant authorities accessing it through national portals linked to this. These could be supplemented by databases at national level to provide access to very large files, with only a link being sent through e-CODEX.

Several possibilities are being considered regarding the platform topology. The Commission could e.g. prepare and provide a ready-made portal (a reference portal) that Member States could install and use as their national portal. Further examination will enable an assessment of the legal feasibility as well as the appropriateness of those possibilities.

To facilitate the exchange of requests in the framework of the European Investigation Order, further work can be done to facilitate the use of Annex A of the EIO Directive, including specification of fields to allow for a choice among options rather than for free text entry; creation of a set of predefined and pre-translated sentences/paragraphs to be used where free text entry is unavoidable; glossaries.

While the focus for the first phase will be on facilitating contacts between authorities in the context of the European Investigation Order, there are also reflections on further uses of the platform in a wider context, for example cooperation with third countries and possibly for direct cooperation with service providers.

3.1.2. Improving cooperation with service providers within the existing framework

The Council conclusions also requested the enhancement of cooperation with service providers. Possible action points identified during the consultation process that might merit further reflection in the coming months to improve direct cooperation between EU law enforcement authorities and U.S.-based service providers for disclosure of non-content data include:

- *Creation of a single point of contact* (SPOC) *on the law enforcement/judiciary side*: A number of Member States, including FI, FR and the UK, have created a central coordinating body for law enforcement requests to service providers based abroad. These bodies gather expertise about the various policies of service providers and build relationships. This facilitates authentication as service providers know their counterpart. It also creates a central "help desk" on service provider policies for law enforcement authorities;
- *Creation of a single point of entry on the provider side*: Current solutions range from standard forms and dedicated mailboxes that are secured and/or closely monitored to specific platforms accounting for national differences and providing targeted advice to law enforcement authorities.
- *Training* on the different policies and procedures of service providers and on the types of data they can provide upon request, either by service providers or by national authorities.
- *Standardisation and reduction of forms used by law enforcement authorities*: Some Member States have already cooperated with service providers to create country-specific forms per service provider that allow for harmonized law enforcement input to the service providers and hence may increase the rates of successful requests.
- *Streamlining of providers' policies*: Service providers could consider streamlining procedures, standards and/or conditions for disclosure of data to law enforcement authorities, e.g. where specific data categories common to several providers are concerned. This would reduce the challenge law enforcement authorities currently face to understand and work with the different policies and procedures and keep up to date with changes and new developments.
- *Establishment of an online platform* to provide comprehensive guidance to law enforcement authorities on current policies, channels, forms, etc.[24] Possible uses of the platform could range from a static repository for service provider policies to an interactive tool guiding law enforcement authorities in identification of the relevant service provider[25] and appropriate channels to use, to a comprehensive tool allowing for the creation and submission of requests to several service providers. The Council of Europe Cybercrime Convention Committee decided on 15 November to maintain an online resource on service provider policies and information on criminal procedural law of States Parties to the Budapest Convention.[26]

---

[24] See for example Council of Europe Budapest Convention on Cybercrime Convention Committee (T-CY), Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, T-CY(2016)5, of 16 September 2016.

[25] See, for example, <www.search.org/resources/isp-list>, which provides contact information and instructions needed to serve judicial process (U.S. domestic) on a number of U.S. ISPs.

[26] Abridged meeting report of the 14-15 November 2016 Council of Europe T-CY 16th plenary meeting, T-CY (2016)32 of 15 November 2016.

3.2. Middle- to long-term solutions

The Council Conclusions also gave a mandate to the Commission to pursue work on facilitating electronic evidence in relation to third countries, for which the recent review of the EU-US Mutual Legal Assistance Agreement and the recommendations it contains will be an important framework. In this context, the Commission has just secured a budget of EUR 1 million under the 2016 Annual Action programme for the Partnership Instrument to finance targeted action to improve EU-US cooperation on cross-border access to electronic evidence.

When it comes to rethinking the existing framework beyond Mutual Legal Assistance procedures, a number of solutions have already been considered preliminarily. These possible solutions can be distinguished between supporting (1) mediated access, i.e. cross-border access to electronic evidence via an intermediary, usually a service provider, and (2) unmediated access, i.e. direct access to data or data that is stored or processed in another country or at an unknown location, including by service providers that do not cooperate with law enforcement authorities.

Possible solutions to facilitate *mediated forms* of cross-border access to electronic evidence will have to take into account current approaches to connecting factors for the exercise of domestic jurisdiction by law enforcement and judicial authorities.

Several experts argued in favour of a multi-factor system that is not restricted to one isolated connecting factor but would rely on several factors alternately or in combination. Additionally, the option of appointing representatives of service providers in the EU in relation to requests for cross-border access to evidence was put forward, e.g. based on the model provided for in Article 27 of the General Data Protection Regulation. As suggested by some of the experts, these solutions could be combined with an obligation to notify other countries that have an interest in a particular request for cross-border access to electronic evidence.

Another option that has been raised, but that will have to be considered carefully in the context of the Digital Single Market, relates to mandating requirements for the location of particular types of data.

Possible solutions to facilitate *unmediated forms* of cross-border access to electronic evidence could be based on direct access for law enforcement and judicial authorities from a computer system to data in another country, or at an unknown location. As indicated here above, there is currently no common approach amongst Member States as regards the use of connecting factors for these measures. As part of the March 2016 conference on Jurisdiction in Cyberspace[27], and as discussed as part of the Commission's expert process possible solutions on direct access could be combined with a notification that builds on Article 32 of the Directive on the European Investigation Order on the interception of telecommunications without technical assistance, which aims to simplify and expedite proceedings by providing that the state concerned must be notified of the measure and can object to it within a specified period of time.

[27] Crossing Borders: Jurisdiction in Cyberspace, Amsterdam, 6-8 March 2016, Preparatory paper of the German delegation: Workshop A "Creating effective MLA processes" and Workshop C "Crime from nowhere; legal challenges for unknown locations".

4. NEXT STEPS

The coming months will be used to further refine the policy options that can be used to address these important issues, in full collaboration with relevant stakeholders including representatives of third countries where appropriate. This non-paper will be used as a basis.

Access to electronic evidence will also be discussed at the EU-U.S. Ministerial Meeting on 5 December 2016, with the aim to launch a regular dialogue at services level that will enable both sides to closely follow the relevant legislative and policy developments in the EU and in the U.S. and identify solutions for practitioners.

As requested by the Council, the Commission will present its findings for the June 2017 Council.[28]

---

[28] Commission Work Programme 2017: Delivering a Europe that protects, empowers and defends, COM(2016) 710 final, chapter 7 on Delivering a Europe that protects, empowers and defends.