144328/EU XXV. GP
Eingelangt am 23/05/17

Council of the European Union

Brussels, 22 May 2017
(OR. en)

9554/17

JAI 526
CYBER 84
COPEN 171
ENFOPOL 259
TELECOM 136
DAPIX 203
COTRA 8
EJUSTICE 69
CATS 58

NOTE

From:	Commission services
To:	Delegations
No. prev. doc.:	9543/17
Subject:	Technical document: Measures to improve cross-border access to electronic evidence for criminal investigations following the adoption of the Council Conclusions on Improving Criminal Justice in Cyberspace

Delegations will find in Annex a technical document prepared by the Commission services on measures to improve cross-border access to electronic evidence for criminal investigations following the adoption of the Council Conclusions on Improving Criminal Justice in Cyberspace.

www.parlament.gv.at

ANNEX

Technical Document:

Measures to improve cross-border access to electronic evidence for criminal investigations following the adoption of the Council Conclusions on Improving Criminal Justice in Cyberspace

This document has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.

www.parlament.gv.at

www.parlament.gv.at

I. Introduction

This paper summarizes the results of the European Commission's expert process on cross-border access to electronic evidence following the 9 June 2016 Council Conclusions on improving criminal justice in cyberspace (hereafter: the *Council Conclusions*).[1]

Cross-border data flows are rising in synch with the growing use of social media, webmail, messaging services and apps to communicate, work, socialize and obtain information. While the great majority of users of these services abide by the law, apps and platforms are also abused for crime and terrorism. Traces of these crimes – commonly referred to as "electronic evidence" – are increasingly available only on private infrastructures. Judiciary and law enforcement authorities use two main investigative tools to obtain access to such electronic evidence for criminal investigations: measures requesting a service provider to provide data on a user of the services ("production requests/orders") and measures allowing direct access to data. As the relevant private sector service providers are often located in other EU Member States or third countries such as the United States (U.S.), the need to access electronic evidence across borders continues to grow.

A number of channels exist for obtaining such cross-border access to electronic evidence. These channels can be based on international law, including the 2001 Council of Europe Convention on cybercrime which provides a framework for mutual legal assistance.[2] EU law also provides avenues, including through the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the EU,[3] replaced as of 22 May 2017 by the 2014 Directive regarding the European Investigation Order (EIO) in criminal matters,[4] and the 2000 Agreement on Mutual Legal

[1] Conclusions of the Council of the European Union on improving criminal justice in cyberspace, 9 June 2016, No 10007/16. This paper is prepared in response to the Council's request for a presentation of deliverables by June 2017.
[2] Council of Europe (Budapest) Convention on Cybercrime (ETS no. 185).
[3] 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.
[4] 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 15 May 2017, only three Member States had communicated national transposition measures.

www.parlament.gv.at

Assistance between the EU and the U.S.[5] In addition, there are a large number of bilateral agreements between Member States and third countries providing for mutual legal assistance (MLA),[6] as well as solutions based on national law. As many of the service providers whose cooperation is required to obtain certain types of electronic evidence are headquartered in the U.S. or other third countries, the internal legal framework of those third countries also applies.

On the basis of these rules, 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 or, where applicable, EIO, 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 the legal framework of the U.S. allows U.S. service providers to directly reply to requests from foreign law enforcement authorities on a voluntary basis, as far as the requests concern non-content data; and
- through direct access from a computer as allowed by different national laws.

These channels suffer from a number of deficiencies (cf. Part II below). Given the increasing volume of cross-border situations, a robust and well-functioning system is needed. Therefore, in its 2015 European Agenda on Security, the Commission committed to address the obstacles.[7] The Council of the EU supported the Commission's commitment in its June 2016 Council Conclusions. It called on the Commission to take concrete actions based on a common EU approach to improve all three channels.

Following the Council Conclusions, the Commission engaged in an extensive stakeholder dialogue to define the problem, set objectives and explore solutions. During the process, Member States' experts, representatives of third countries, representatives of industry associations, service providers, civil society organisations and academics provided comprehensive input. Specific proposals for approaches and measures were also put forward and presented by various stakeholders, including experts from Belgium and Germany.

[5] 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.
[6] See for instance the Treaty between the Kingdom of the Netherlands and the United States of America on mutual assistance in criminal matters of June 1983.
[7] COM(2015) 185 final.

www.parlament.gv.at

This paper sets out a more comprehensive problem definition, building on the December 2016 Progress Report[8] to the Council, corresponding objectives, and possible solutions that have emerged from the expert process, grouped under (a) practical measures to improve the use of existing legal frameworks (Part III.A.), and (b) possible policy options to reform the existing legal framework where the expert process has revealed deficiencies (Part III.B.). In parallel, the Commission will also report to the Council on 8 June 2017 on the practical measures and possible options for legislation that are contained in the present document in a Non-paper.[9]

The measures described hereafter are not mutually exclusive and can be combined where relevant. The implementation of practical measures does not exclude legislative measures[10] and vice versa, and measures can complement each other, should a decision be taken to consider both practical and legislative measures.

II. Problem Definition

In its December 2016 Progress Report[11] to the Council, the Commission presented a first overview of problems in relation to the three strands identified in the Council Conclusions.

A. Summary of December findings

In relation to the **cooperation between law enforcement and service providers**, the Commission described the main concerns raised by various stakeholders, including on the transparency of the process, the reliability of stakeholders, their accountability, the identification and contacting of relevant service providers, the determination of the authenticity and legitimacy of a request from an authority, the unequal treatment of authorities across Member States and the admissibility of evidence obtained in court proceedings.

On **mutual legal assistance and mutual recognition**, the Commission described as main issues the length of time for processing a request, the resource-intensity and complexity of the process and the lack of transparency.

[8] European Commission Progress Report to the Council of the European Union, ST 15072/1/16.
[9] Non-paper from the Commission services, *Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward.*
[10] Soft law instruments, such as codes of conduct, might be also considered.
[11] Cf. fn. 8.

www.parlament.gv.at

Finally, in relation to **enforcing jurisdiction in cyberspace**, the Commission highlighted the added complexity created by different and at times conflicting approaches taken by Member States on the scope of investigatory measures online, notably as regards the factors allowing an authority to use those measures despite potential effects on another country's territory (i.e. connecting factors), the enforcement of those measures and situations where it is not possible to determine where such effects might actually take place.

B. Further development of the problem definition

This problem definition was validated and further refined in the expert process to provide a more robust basis for identifying possible solutions.[12] Based on stakeholder input, the Commission has identified additional aspects. These can be summarized as follows:

1. Horizontal challenges

A fundamental challenge highlighted by stakeholders across all three channels to access electronic evidence lies in the fact that stakeholders and legal frameworks disagree as to **what constitutes a "cross-border" situation**. Some laws use the storage location of the data in question as a connecting factor, others use the location of the seat of a potential addressee of an order and yet others rely on a domestic business presence of the potential addressee.

A number of laws even employ **different connecting factors depending on the type of data**, usually granting larger domestic competences for non-content data than for content data. This creates a significant challenge for international comity – for example, country A may perceive an action by country B as having a cross-border dimension affecting its territorial interests while country B regards the situation as purely domestic in nature; both countries will thus also disagree on the need to use domestic or cross-border channels to obtain the evidence concerned.[13]

[12] The meetings with industry association, service providers and civil society organisations have been organised in the context of the **EU Internet Forum**.

[13] Cf. the discussion in Microsoft Corp. v United States, U.S. Court of Appeals for the Second Circuit, Docket No. 14-2985. Cf. also the Skype Belgian case law: Belgian authorities considered the request for data as a domestic request when the Provider located in Luxembourg considered the request as a foreign request (in accordance with the current Luxemburgish legal framework).

www.parlament.gv.at

Accordingly, service providers active in multiple countries highlighted **conflicting interests** of those different countries. It was not always obvious to them which legal regime applied. They also considered that unilateral developments in some Member States were harmful as they caused additional ambiguity.

Furthermore, there is **no common understanding of how to categorize specific types of electronic evidence**. Electronic evidence is frequently categorized as follows: (1) basic **subscriber information** (allowing identification of the subscriber to a service); (2) information relating to the provision of services, referred to as **traffic, meta** or **transactional data**; and (3) **content data**.[14] While some service providers consider the IP address used at the time of creation of an account as basic subscriber information, others view it as transactional data. Other types of electronic evidence for which no legal definitions are available may also be of relevance for criminal investigations, including types of evidence that are not necessarily related to communications. Data from all of these categories is personal data as far as it allows for the identification of an individual.[15]

---

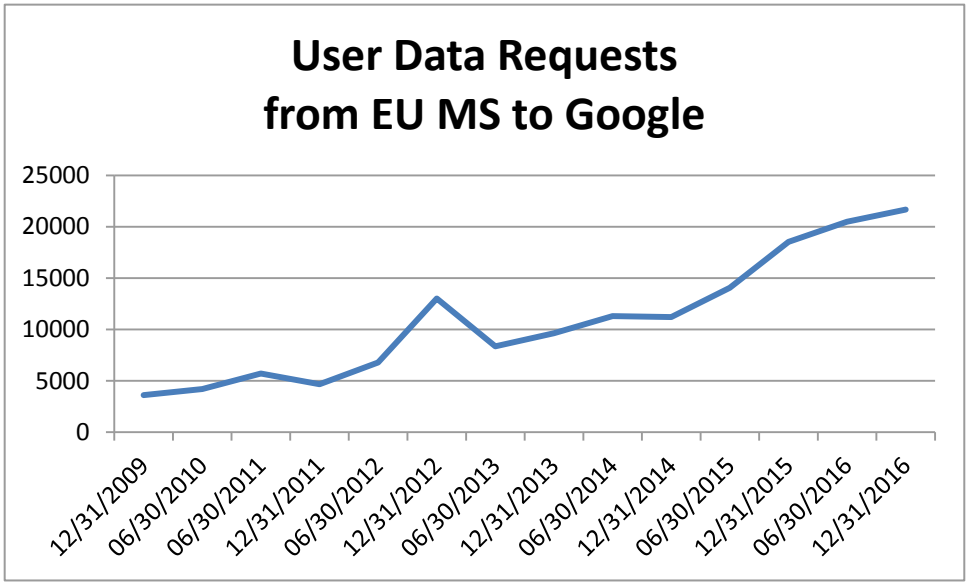
[14] One **definition** of **subscriber information** is: "any data held by a service provider, relating to subscribers of its services other than meta-data or content data and by which can be established: i) the type of communication service used, the technical provisions taken thereto and the period of service, ii) b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement, iii) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement", cf. Article 18(3) of the Council of Europe Budapest Convention on Cybercrime. One **definition** of **communications meta-data** is: "data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication", cf. Article 4(3)(c) of the proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final. Together, subscriber data and meta-data can be referred to as non-content data. One **definition** of **communications content data** is: "the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound", cf. Article 4(3)(b) of the proposal for a Regulation on Privacy and Electronic Communications. According to the results of the September 2016 questionnaire, 12 Member States indicated they use a definition of subscriber information (AT, RO, SE, EL, LV, DE, DK, ES, FI, PT and UK), 15 Member States indicated they use a definition of traffic information (AT, RO, SE, BE, SK, EL, LV, DE, DK, ES, FI, PT, SI, UK and LT), and 8 Member States indicated they use a definition of content information (AT, RO, EL, DE, DK, ES, FI and FR). Member States also have different definitions of types of electronic evidence in their legal framework, sometimes on the basis of international conventions or EU acquis, which may hamper cross-border access to electronic evidence for criminal investigations.

[15] Personal data is any information related to an identified or identifiable natural person, Article 4(1) General Data Protection Regulation (EU) 2016/679 (GDPR).

www.parlament.gv.at

The absence of certainty as to which category applies can lead to an **uneven application of procedural safeguards**, as legal procedures and safeguards vary across different categories of electronic evidence. The lack of consistent definitions of different types of data may also result in conflicts of law as regards the scope of measures. At a more practical level, it may lead to misunderstandings between requesting authority and executing authority or service provider addressed.

In terms of practical challenges, the need for cross-border access to evidence continues to grow, as evidenced by the mounting volume of requests made in spite of the shortcomings of the current system. By way of example, the requests from EU Member States' authorities to one service provider (Google) may serve as illustration:



The volume rose from a total of 3,609 requests from nine Member States during the six months ending on 31 December 2009 to 21,668 requests from 27 Member States for the six months ending on 31 December 2016, an average increase of 19% per year and an overall increase of 500% over the seven-year period.[16] Important increases also affect MLA proceedings.[17]

[16] Based on data from the Google transparency reports. Until 30 June 2014, the reports do not differentiate between standard access requests, emergency requests and preservation requests. Later figures are based on standard access request statistics only.
[17] Cf. Section 3 below with illustrations of MLA requests to the U.S.

www.parlament.gv.at

Besides the larger service providers which have often already established a range of different channels and policies to deal with requests, there is also a growing number of smaller service providers and a plethora of apps that can become relevant in criminal investigations. In these situations, experts highlighted that cooperation often was more challenging because both sides were unfamiliar with each other, there was a lack of specific rules and policies, and a lack of familiarity with the framework.

2. Direct cooperation

In relation to direct cooperation between authorities and service providers, in particular when the service provider is outside the domestic jurisdiction, the key additional issues identified were the following:

Stakeholders highlighted the need to ensure **the protection of rights to privacy** and provide measures to that extent, including user notification. The majority of providers underlined the importance of user notification, which should only exceptionally be deferred or prohibited.[18] Any such exceptions should be specific and not provide for indefinite blanket coverage. Service providers also indicated that it is often unclear to them from law enforcement requests and applicable rules whether they are allowed to notify a customer, and if not, whether a law enforcement authority will do it and under which conditions.

Transparent information and fair processing are core principles of EU data protection rules; access, rectification and erasure rights are also guaranteed. However, restrictions might be imposed by way of legislative measures to safeguard, inter alia, public security or the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties.[19]

Also in relation to privacy and data protection, stakeholders from the private sector also highlighted the specific expectations of **corporate customers** that a provider of corporate systems and services should in principle not be asked to provide information of the corporate client's. Rather, it was pointed out, authorities should consider requesting the information from the corporate client.

[18] Under U.S. legislation (the Electronic Communications Privacy Act (ECPA)), authorities are obliged to notify, and service providers are allowed to notify, unless a court order imposes a temporary block on notification.
[19] Article 23 of the Regulation 2016/679 and Article 13(3) of the Directive 2016/680

www.parlament.gv.at

While most Member States' laws also attach importance to the **location** where relevant data is **stored**, this has proven very difficult in practice as a connecting factor.[20]

While service providers usually receive some form of **cost reimbursement** in relation to requests made in the domestic setting, notably domestic providers of telecommunications services, this is different when considering cross-border requests. Several U.S.-based service providers indicated that they currently respond to law enforcement requests without asking for a reimbursement of related costs.[21] Linked to this, some stakeholders have stressed that smaller companies may struggle to meet requirements that larger companies might be able to meet comparatively easily because of their scale. In relation to possible new obligations, it was pointed out that service providers might incur unforeseen expenses. Some stakeholders suggested that a requirement for a reimbursement of costs could also be seen as a safeguard to ensure that the authorities' requests are limited to the absolute minimum.

3. Mutual Legal Assistance (MLA) with third countries

In relation to mutual legal assistance, stakeholders provided more details on the current challenges. These relate in particular to the time frame, as already outlined in the December Progress Report: Requests for mutual legal assistance take between one and 18 months. The MLA mechanism is complex and diverges from country to country.

[20] For example, while Facebook operates a large data centre in northern Sweden, Sweden has always been asked to send its request to Facebook's headquarters in the United States.
[21] Republic of Austria.

www.parlament.gv.at

These formal procedures ensure that the right authorities are involved and that appropriate safeguards are taken into account when there is a sovereign interest of more than one country. They also have the consequence that requests for mutual legal assistance require considerable time to be processed, even in cases with little or no connection to the receiving country besides the seat of the service provider.[22] The legal framework is fragmented and complex; practitioners are faced with a high number of bi-lateral and multi-lateral conventions and with the specific requirements of recipient countries' legal systems. For example, for requests addressed to the U.S., the *probable cause* requirement has to be met to allow the disclosure of content data, which is a concept foreign to EU practitioners, who sometimes struggle with it.[23]

As highlighted already in the December Progress report, the EU-U.S. MLA Review Report of 2016 underlines that delays are due to bottlenecks at the phase of the reception of requests by the U.S. Authorities and also during the execution phase. This is mainly due to the steep and sustained increase in volume of requests; as the U.S. authorities reported already in 2014, "[o]ver the past decade the number of requests for assistance from foreign authorities handled by the Criminal Division's Office of International Affairs (OIA) has increased nearly 60 percent, and the number of requests for computer records has increased ten-fold."[24] In an effort to improve the situation, the U.S. Department of Justice has created a dedicated team for electronic evidence and has obtained a change in legislation allowing them to make the relevant pleas before the local District of Columbia courts. Nonetheless, the resources continue to be outmatched by the swift growth in requests.

More recently, bottlenecks have also been reported with regard to Ireland, where many service providers have European headquarters or data centres.

---

[22] While data location is often cited as the key factor in determining territorial competence, in practice it is impossible to tell for authorities where the data is stored without the cooperation of service providers. Therefore they can only direct mutual legal assistance requests at a given country once the service provider has disclosed the data storage location and has agreed to keep the data in place, i.e. not to move it to another jurisdiction. Service providers may also choose to "shard" their data, storing bits in various locations, and some have internal technical measures and policies allowing access to data only from one country regardless of whether it is stored there or – wholly or in part – in other countries. Cf. U.S. District Court for the Eastern District of Pennsylvania, In re Search Warrant No. 16-960-M-01, p. 7 and 8, for further details.

[23] The EU-U.S. Review Report finds that one of the main reasons for Member States requests not being successful is that they do not meet the US probable cause requirements.

[24] https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf

www.parlament.gv.at

4. Enforcement of jurisdiction in cyberspace

Regarding **direct access**, while most Member States appear to allow for their authorities to access an information system as part of an extended search (i.e. in the context of an open search of a device of a suspect or witness), only a few Member States allow their authorities to perform remote searches (i.e. a search from an authority's computer, usually not disclosed to the target until later), although the number is increasing.[25]

The expert consultation process found that, in a situation of a loss of knowledge of data location, several Member States assume that the direct access takes place in a purely domestic context and permit access to data, e.g. for copying.[26] However, other Member States take the opposite approach and assume that the data is elsewhere and that access may have an effect in another country (although the data might in fact be domestically available).[27] On the basis of the expert consultation process, Member States also appear to have different approaches concerning the conditions and safeguards applicable to the use of direct access. These concern the context of the investigative measure, and the purpose for which it can be used.

While this diversity may reflect different legal cultures, it becomes an issue when a Member State allows its authorities to access data in a way that is perceived by another Member State as affecting its sovereignty/territoriality. Moreover, the level of rights of the persons whose data is accessed also varies considerably, depending on which Member State is performing the investigative measure.

[25] Study for the LIBE Committee on the "Legal Frameworks for hacking by law enforcement: identification, evaluation and comparison or practices", 2017.
[26] In response to the September 2016 questionnaire, at least 4 Member States indicated that law enforcement and judicial authorities can access electronic evidence directly if it is unclear or even impossible to establish where the information is located (BE, ES, PT and FR).
[27] In response to the questionnaire, 8 Member States indicated that their authorities cannot themselves access electronic evidence when it is unclear what the location of the information is or when it is impossible to establish the location of the information (HU, SE, HR, CY, EL, LV, FI and SI) and 11 Member States clarified that this depends on specific circumstances (AT, EE, RO, SK, NL, CZ, DE, DK, UK, IT and LT).

www.parlament.gv.at

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

To address the problems outlined above, the expert process helped identify a number of practical measures that could improve the cooperation between authorities and service providers, and the cooperation among judicial authorities.

A. Improving cooperation with service providers

1. Objectives

On the basis of the problems identified in the expert process, the following objectives can be established for improving cross-border access to electronic evidence on the basis of direct cooperation with service providers[28] by means of practical measures:

- To improve the transparency of direct cooperation between authorities and service providers;
- To improve the reliability of direct cooperation;
- To reduce the heterogeneity of rules and the resulting complexity;
- To improve accountability on both sides;
- To facilitate identifying and contacting service providers;
- To facilitate assessment of authenticity and legitimacy of authorities' requests;
- To improve equal treatment of requests by service providers across Member States.

[28] 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 2702 of the Stored Communications Act (SCA) under 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.

www.parlament.gv.at

2. Practical measures

The following practical measures for the cooperation between law enforcement or judicial authorities and service providers to obtain cross-border access to electronic evidence are considered in the context of the existing legal framework, which mostly provides for cooperation on a voluntary basis.[29] Given the applicable legal framework in the Member States and third countries, this type of direct cooperation currently mostly takes place with service providers whose headquarters are in the U.S.. These service providers can voluntarily provide **non-content data**[30] directly to foreign law enforcement upon request, pursuant to § 2702 of the U.S. Electronic Communications Privacy Act; they are prohibited from providing content data except in cases of emergency. For non-content data, this voluntary channel has de facto become the main channel for obtaining cross-border access to electronic evidence for criminal investigations.

The importance of improving direct cooperation between law enforcement and judicial authorities and service providers, as well as its complementarity with other channels to obtain cross-border access to electronic evidence, was recognised by the June 2016 Council Conclusions, and is reflected by the significant number of requests that are made to service providers.[31] In addition, the importance of the channel was underlined during the expert consultation process by most of the Member States and other stakeholders, including service providers. On the basis of the expert consultation process, the following practical options received broad support to improve cross-border access to electronic evidence.

[29] Which means that there is a domestic legal title which cannot be enforced directly in the recipient country. Nevertheless, it should be taken into account that the distinction between voluntary and mandatory cooperation is not always easy to establish, and in fact, in the absence of a clear legal framework both parties involved may disagree on the voluntary or mandatory nature of the direct cooperation.

[30] Vis-à-vis EU law enforcement authorities, given that it is a voluntary system from the perspective of U.S. laws, each U.S. provider decides what kind of non-content data would be disclosed following a direct request.

[31] According to a report from the Convention Committee of the Council of Europe Budapest Convention on Cybercrime (T-CY) and on the basis of service provider's transparency reports, in 2014 Parties to the Convention other than the U.S. sent 109.000 of these production requests to six major service providers headquartered in the U.S. (Apple, Facebook, Google, Microsoft, Twitter and Yahoo), "Criminal justice access to data in the cloud: Cooperation with “foreign” service providers - Background paper prepared by the T-CY Cloud Evidence Group", 3 May 2016, T-CY (2016)2.

www.parlament.gv.at

First, the creation of a **single point of contact (SPOC)** on the law enforcement authorities' side in the Member States, as it could significantly improve the direct cooperation between those authorities and service providers. Currently, a number of Member States (FR, UK, SE, BE, FI, LT) have already created a central coordinating body for the direct cooperation between law enforcement authorities and service providers. These SPOCs provide expertise on the different policies of service providers and can establish relationships with service providers, which for example facilitates the authentication of requests. The centralisation of expertise also improves the quality of outgoing requests; some but not all SPOCs also validate each request before it is transferred. The establishment of SPOCs has resulted in a significant improvement in the efficiency of this channel, both on the side of the authorities in the Member State, and on the side of the service provider. Although not all Member States would have to choose the exact same implementation of SPOCs in their system, e.g. at central or decentralised level, the Commission could consider giving recommendations to facilitate their implementation and the development of best-practices.

Second, the creation of a **single point of entry on the service provider's side could also** improve the direct cooperation between those authorities and service providers. Currently a number of major service provider have already established standard forms, dedicated mailboxes or specific electronic platforms accounting for national differences and providing targeted advice to law enforcement and the judiciary to facilitate the use of this channel, including e.g. service providers like Facebook, Microsoft, Twitter and Google. These practical measures have resulted in significant improvements of the direct cooperation between those service providers and law enforcement authorities, both in terms of reliability and efficiency. Nevertheless, not all service providers have implemented these measures and more could be done to ensure a common approach amongst service providers. The Commission could further explore opportunities with service providers on a voluntary basis.

www.parlament.gv.at

Third, it has been raised that significant improvements could be made through **streamlining service providers' policies** on cross-border access to electronic evidence. Given that there is no legal framework in place, currently all service providers are free to choose whether and on what terms they provide access to non-content data. The development and application of harmonised procedures, standards and conditions could facilitate the direct cooperation between law enforcement and judicial authorities and service providers. A harmonisation of procedures, standards and conditions could bring unity in current approaches that sometimes appear to differ widely. Streamlining of procedures, standards and conditions would provide for less confusion and more efficient requests at the side of law enforcement authorities. Although different business models and infrastructures used by service providers may not allow for a full harmonisation of policies, the Commission could further explore opportunities with service providers on a voluntary basis.

Fourth, it has been indicated that the **standardisation and reduction of forms** used by law enforcement and judicial authorities could enhance the direct cooperation between those authorities and service providers. Some Member States (**FR, HU, SE**) have already cooperated with service providers to create and implement such forms, taking into account the requirements from a national criminal procedural law perspective and the service provider's perspective, e.g. as based on applicable law of other related countries, which has resulted in the improvement of the functioning of this channel. In some cases this has resulted in a significant reduction in the number of forms used. Depending on the specific requirements of the national criminal procedural law, and the different business models and infrastructures used by service providers, it could be conceived to develop forms that would allow for harmonised law enforcement input to service providers. The Commission could facilitate the development of these standardised forms by national authorities and service providers on a voluntary basis.

www.parlament.gv.at

Fifth, all stakeholders have indicated that additional **training for law enforcement and judicial authorities** could support the functioning of direct cooperation between those authorities and service providers. Training activities could provide for a better understanding of different policies and procedures used by service providers, and a common understanding of other countries' law concepts and technical capabilities might enhance responses. As part of the expert consultation process, it has been suggested that training should not be fragmented per country but could rather be centralised to ensure for synergies. The Commission could facilitate the development of training programmes in full collaboration with national authorities and service providers on a voluntary basis. The Commission has made available €1 million to fund related activities targeting the relationship with the U.S. in particular under the Partnership Agreement[32], of which €500.000 are available for improving direct cooperation with service providers.

Sixth, several stakeholders have suggested considering the **establishment of an online information and support portal** at EU level to provide support to online investigations, including information on applicable rules and procedures. A number of initiatives pursue that aim, in particular efforts under the **Council of Europe Budapest Convention on Cybercrime** and elsewhere to create repositories of the different provider policies,[33] and Europol's work on the establishment of the **SIRIUS portal** to facilitate online investigations, including the direct cooperation between authorities and service providers[34].

[32] Commission implementing decision modifying the 2016 Partnership Instrument Annual Action Programme for cooperation with third countries to be financed from the general budget of the European Union, C(2016) 7198 final, annex 18 (Action Fiche for International Digital Cooperation).

[33] A static repository of countries' regulatory frameworks and procedures has been developed in the context of the Council of Europe Budapest Convention on Cybercrime. See T-CY Cloud Evidence Group, "Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY", 16 September 2016. There are also a number of other services available; see, for example, www.search.org/resources/isp-list, which provides contact information and instructions needed to serve judicial process (US domestic) on a number of US-based or headquartered service providers.

[34] Europol has started work on an interactive platform allowing law enforcement authorities to collect publicly available information, to identify the relevant service providers for additional information, and to find the appropriate channel for making the request.

www.parlament.gv.at

Although these practical measures would significantly facilitate the direct cooperation between law enforcement and judicial authorities and service providers, it should be acknowledged that none of these measures will solve all problems identified. They will facilitate the cooperation with U.S. service providers under the current U.S. legal framework for direct access to non-content data, which would already cover a large number of requests, but this is also their limit. Within the EU, direct cooperation is not used as a channel for cross border access to electronic evidence between law enforcement and judicial authorities and service providers headquartered in other EU Member States, even though practitioners from law enforcement and the judiciary see a growing need. This need stands to increase further with the abolition of roaming costs as a result of which consumers are increasingly likely to use service provided by companies established in another Member State. In addition, all these options depend on the willingness and commitment of service providers to cooperate, as direct cooperation is a voluntary mechanism.

Finally, none of these measures will solve the issue of fragmentation linked to the divergent practices and policies of service providers and EU Member States: they will not be sufficient i) to provide to EU citizens/residents the same standard of transparency and rule of law regarding the disclosure of their data, which depend on the conclusion and the content of agreements between their Member State(s) and their provider(s); ii) to reduce the different approaches among private companies offering the same services, as the legal framework and obligations vis-à-vis law enforcement/judicial authorities depend on their nationality (EU or US) and their statute (internet providers or telecom).[35]

[35] In this regard, the on-going revision of the e-Privacy framework, which proposes to introduce the requirement to designate a representative in the Union for service providers not established in the Union offering services to end-users in the Union and to enlarge its scope from telecom to OTT, will have to be taken into account.

www.parlament.gv.at

On the basis of the expert consultation process, the implementation of practical measures should be pursued to improve cross-border access to electronic evidence on the basis of direct cooperation between authorities and service providers, where relevant in the context of the EU Internet Forum.

- *The establishment of Central Points of Contact (SPOCs) in Member States,*
- *The use of a single point of entry at the side of service providers,*
- *The streamlining of service provider's policies,*
- *The standardisation and reduction of forms used in Member States,*
- *The development of training programmes for law enforcement and judicial authorities,*
- *The establishment of an online information and support portal at EU level.*

B. Improving cooperation among judicial authorities

1. Within the EU

As of 22 May 2017 Directive 2014/41/EU on the EIO will replace the existing fragmented legal framework relating to the collection and transfer of evidence between EU Member States[36] by a system of judicial cooperation based on mutual recognition. It aims to make cross-border investigations faster and more efficient by setting out mandatory deadlines and limited ground for refusal. This will to some extent improve the expediency of proceedings, which is the major issue outlined by Member States regarding judicial cooperation channels.[37] However, regarding Ireland and Denmark, which are not participating in the EIO and regarding third countries (notably the U.S.), the request of investigative measures will continue to be based on MLA channels

[36] Notably the European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of 20 April 1959 and its two additional protocols, bilateral agreements, provisions of the Schengen Agreement, Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and its protocol.

[37] 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 three Member States had communicated national transposition measures.

www.parlament.gv.at

a) Objectives

On the basis of the expert consultation process, the following objectives have been identified for improving cross-border access to electronic evidence on the basis of cooperation between judicial authorities:

- To improve the expediency of judicial cooperation requests for access to electronic evidence;
- To improve the transparency of the process;
- To reduce the complexity and resource-intensity of such requests.

b) Practical measures

In accordance with the mandate given by the Council Conclusions, the Commission has started work on an **electronic user-friendly version of the form set out in Annex A of the EIO Directive** to request the securing and obtaining of e-evidence, to facilitate completion and translation of the form.[38] It will also include guidance that allows practitioners to fill it in without having followed dedicated training. 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 for consultation of Member States. This electronic form will be made available on the EJN website, and it will later be incorporated into the platform mentioned below;

Following the Council's request for **a secure platform for the online exchange of electronic evidence between EU judicial authorities**, the Commission has also progressed in defining the parameters of such platform, in consultation with the Member States.[39] Based on the feedback received during several meetings with Member States and to a letter, the Commission proposes to set up a decentralised system and to provide a reference portal and storage capacity for those Member States who presently don't have this capacity, which they can then install nationally.

[38] This work does not imply a modification of the form, but e.g. pre-defined scroll-down menus to select from.

[39] This platform is currently considered to cover the exchange of e-evidence among EU judicial authorities on the basis of the Directive regarding the European Investigation Order. However, in a longer term perspective an extension of the IT platform to facilitate direct cooperation between law enforcement authorities and service providers could be considered (III.A.1. above), as well as to cooperation with judicial authorities of third countries.

www.parlament.gv.at

Throughout the meetings, a majority of Member States expressed the choice to use e-CODEX as the tool for the secure transmission of the data.[40] As the setting up of the system requires (parallel) work by Member States and Commission a dedicated project team including representatives of all Member States is being set up. At a meeting on 13 March 2017 both the organisation of the project and a tentative calendar were discussed with Member States. According to the present timeline the system could be operational by the summer of 2019.

The setting up of this platform, together with the form, is expected to facilitate judicial cooperation and the exchange of information between judicial authorities of Member States participating in the EIO, allowing them to secure and obtain e-evidence more quickly and effectively, whilst fulfilling the necessary security requirements in a user-friendly manner. They will be able to identify the relevant authority more quickly, fill in the form more easily and transmit it in a faster and more secure way as is currently the case. The tool can also be used to send the evidence requested back. Thereby, the process should become faster, and to some extent, less resource-intensive and less complex. The use of the IT platform will also increase the transparency of the process, allowing for statistics to be collected and for better information as to the stage of the procedure.

However, the benefits of these solutions will be limited to EU Member States participating in the EIO. The mutual recognition process, including its deadlines, will not be fundamentally changed, meaning that the process will remain long and more resource-intensive when compared to direct cooperation with service providers.

On the basis of the expert consultation process, and in cooperation with Member States, work on the electronic form and the secure platform to exchange requests for electronic evidences should be continued with the aim to improve cross-border access to electronic evidence on the basis of the EIO between EU Member States.

[40] The Commission has launched an assessment of the impact of various options for maintaining e-CODEX in the long term, which includes examining the need for a legal basis.

www.parlament.gv.at

2. *Beyond the EU*

a) Objectives

The expert consultation process identified the following objectives for practical measures to improve cross-border access to electronic evidence through cooperation between judicial authorities:

- To improve the expediency of judicial cooperation requests for access to electronic evidence;
- To reduce the complexity and resource-intensity of such requests.

b) Practical measures

Cross-border access to electronic evidence on the basis of judicial cooperation could be improved through closer cooperation with the U.S. authorities, as many service providers are headquartered or have a seat in the U.S.. In the same vein, cooperation with the U.S. could also be used to facilitate the channels of direct cooperation with service providers.

The EU and the U.S. already established an Agreement on Mutual Legal Assistance, [41] which was reviewed in 2016. The Review Report contains recommendations concerning electronic evidence, notably that EU Member States may seek to obtain direct cooperation from U.S. service providers 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.

In line with these recommendations, the following measures have been identified during the expert consultation process:

[41] 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.

www.parlament.gv.at

Firstly, cross-border access to electronic evidence could be improved by means of **regular technical dialogues with the U.S. Department of Justice**, also in the longer term. In order to ensure a common approach and to avoid conflicts of law, both the EU and the U.S. could benefit from a closer collaboration, including through visits, to work on practical aspects but also to discuss legislative developments on both sides of the Atlantic. Applicable law in the U.S. is currently subject to review, and conflicting legislative approaches between the EU and the U.S. should be avoided. At the December 2016 EU-U.S. Justice and Home Affairs Ministerial meeting, it was already agreed to step up the collaboration on cybercrime, including on cross-border access to electronic evidence.[42]

Second, it has been found that **regular contacts between the EU Delegation to the U.S., the Commission and liaison magistrates** of Member States in the U.S. could improve cross-border access to electronic evidence. As part of the expert consultation process, the Commission and the EU Delegation to the U.S. have already facilitated a number of meetings, which provided for an opportunity to share experiences and to learn about practical problems liaison magistrates of Member States are facing in their day-to-day work on cross-border access to electronic evidence, both on the basis of direct cooperation and on the basis of mutual legal assistance procedures. The Commission and the EU Delegation could continue to facilitate such regular contacts.

Third, it has been suggested that an **exchanges of best practice and further training** for EU practitioners on applicable rules in the U.S. could improve cross-border access to electronic evidence. Best practices could be developed and exchanged and further training could be developed in relation to U.S. legal concepts, including the criterion of probable cause relevant for access to content. The Commission is making available €500.000 for this purpose under the Partnership Agreement[43].

[42] Joint EU-US statement following the EU-US Justice and Home Affairs Ministerial meeting of 5 December 2016, Doc. 722/16.

[43] The Commission launched a call for proposals with a budget of €1mln total for improving cooperation both between judicial authorities of EU Member States and the U.S. and between EU authorities and U.S.-based service providers on 4 May 2017 under the Partnership Instrument Annual Action Programme 2016 Phase II - International Digital Cooperation - Component D – Cross Border Access to Electronic Evidence (EuropeAid/155907/DH/ACT/Multi). More information is available at http://ec.europa.eu/europeaid/about-funding_en.

www.parlament.gv.at

These options for practical measures would facilitate cross-border access to electronic evidence held by U.S. companies for criminal investigations on the basis of direct cooperation and mutual legal assistance. By allowing the identification of existing issues and discussions on possible ways to solve them, they would allow to make the process more efficient. Their scope would be limited to U.S.-based service providers. It should be further acknowledged that many of these improvements depend on the goodwill of the U.S.[44].

Beyond the U.S., further bilateral cooperation with Member States of the European Economic Area and with third countries such as Canada could also be envisaged.

On the basis of the expert consultation process, cooperation should be continued with the U.S. to improve cross-border access to electronic evidence on the basis of mutual legal assistance procedures:

- *Regular technical dialogues with the U.S.,*
- *Facilitate regular dialogues between the EU Delegation to the U.S. and liaison magistrates of Member States in the U.S.,*
- *Funding for the exchange of best-practices and training for EU practitioners as regards the applicable rules in the U.S.*

IV. Legislative measures and international agreements to improve cross-border access to electronic evidence

The proposed practical solutions discussed above could contribute to significantly improving cross-border access to electronic evidence, both with regard to U.S. service providers regarding non-content data, and within the EU with regard to the functioning of the EIO. They could already present certain results within a reasonable time frame.

[44] The option to develop a standardised form for MLA requests was also envisaged and proposed to the US, but not pursued notably because it would not solve the major issue faced by EU practitioners concerning the demonstration of the "probable cause" principle. It should be acknowledged that the possibility to standardise the "probable cause" requirement is very limited as the demonstration has to be done case by case and, in application of the U.S. common law legal framework, part of the relevance of the demonstration depends on the jurisprudence of each judge. Regarding the demonstration of probable cause U.S. , trainings and guidance may be more adapted than standardisation.

www.parlament.gv.at

On the other hand, they 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, a number of legislative measures could also be considered. These are set out in general terms here below, listing the various considerations that would need to be taken into account if a decision is taken to proceed with defining concrete legislative proposals. Such legislative proposals would be subject to an impact assessment, which would include their legal feasibility under the relevant provisions of the TFEU, notably Article 82, and a public consultation.

All measures proposed below should ensure a high level of protection of fundamental rights and of rights in criminal proceedings, including the right to judicial redress.

A. Types of electronic evidence

One aim identified during the expert consultation process was to improve cross-border access to electronic evidence by means of the establishment of a common interpretation of types of electronic evidence. It would facilitate mutual understanding, but also determine the scope of legislative measures to provide for production requests and orders, and direct access.

1. Objective

- To provide legal certainty on definitions of several types of electronic evidence.

2. Possible measures

On the basis of the expert consultation process, the the following measure could improve cross-border access to electronic evidence.

www.parlament.gv.at

Measure to provide for a common understanding and harmonised definitions of types of electronic evidence at EU level

The measure would define specific categories of electronic evidence by means of legislation at EU level.

In addition, a library at technical level could be provided to facilitate a common understanding at EU level of the technical elements to be considered as part of those legal categories.

The measure would thus combine general categories set out in legislation and a more specific mapping provided by the technical library.

The measure would harmonize definitions of electronic evidence on the basis of a legal proposal, in order to harmonize the scope for investigative measures available to obtain cross-border access to electronic evidence. In addition, harmonization would also create legal certainty for stakeholders addressed by these investigative measures, including by production requests and production orders.

Experts suggested that the categories of data (subscriber information, traffic information and content information) could be further harmonised while taking into account the definitions of the types of electronic evidence currently in place e.g. in the Council of Europe Budapest Convention on Cybercrime, the current e-Privacy Directive and the proposal for an e-Privacy Regulation.[45] On the basis of the expert consultation process, it has also been suggested that other types of information, beyond information related to communications, should also be considered.

Such definitions of electronic evidence may have to take into account the entity the information is collected from, e.g. the type of service provider, as well as the measure used to obtain the information, e.g. by means of a production request/order or interception.

[45] See the proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final

www.parlament.gv.at

Several stakeholders underlined the need to develop definitions that are future-proof in order not to be affected by technological developments. For that purpose, a library could be developed at technical level of information elements of types of electronic evidence.

The technical library could be developed in cooperation with Member States' authorities and service providers on a voluntary or co-regulatory basis. It could strive to be comprehensive or, in the alternative, limit itself to mapping data points that are considered to be on the border between two categories to provide clarity in those situations where the interpretation among different authorities and service providers varies at present.

B. Streamlining production requests/orders

The expert process highlighted the need to streamline and harmonise requests from law enforcement or judicial authorities to service providers for the production of user data.

For the purposes of considerations here, **production requests** are non-mandatory requests made by a law enforcement or judicial authority in one Member State to a private third party (usually a service provider) in another country to provide data under its control. The service provider can voluntarily provide the requested information. If the request is not complied with, there is no possibility of enforcement. Although voluntary in nature, the importance of this channel for obtaining cross-border access to electronic evidence was recognised by the June 2016 Council Conclusions, and is reflected by the significant number of requests that are made to service providers.[46]

[46] According to a report from the Convention Committee of the Council of Europe Budapest Convention on Cybercrime (T-CY) and on the basis of service provider's transparency reports, in 2014 Parties to the Convention other than the U.S. sent 109.000 of these production requests to six major service providers headquartered in the U.S. (Apple, Facebook, Google, Microsoft, Twitter and Yahoo), "Criminal justice access to data in the cloud: Cooperation with “foreign” service providers - Background paper prepared by the T-CY Cloud Evidence Group", 3 May 2016, T-CY (2016)2. Also see above at II.B.2 for an example of requests from EU Member States to one service provider.

www.parlament.gv.at

Given the applicable legal framework in the Member States and third countries, this type of direct cooperation on the basis of production requests currently mostly takes place with service providers headquartered in the U.S., where legislation allows service providers to voluntarily provide non-content data (subscriber information and traffic information) to foreign law enforcement authorities upon request.[47]

In contrast to the non-binding requests, **production orders** are mandatory instructions by law enforcement and judicial authorities to a third party to provide data under its control. They are directly enforceable on the territory of the Member State in which they are issued. They differ from the production requests mentioned above by their mandatory nature.

1. Objectives

On the basis of the expert consultation process, the following objectives have been identified for improving cross-border access to electronic evidence on the basis of a production request or production order by means of a legislative measure:

- To protect fundamental rights;
- To improve the reliability of direct cooperation between authorities and service providers in cross-border cases;
- To improve the accountability of authorities and service providers in direct cooperation;
- To reduce administrative burden;
- To foster a common understanding on minimum conditions and safeguards;
- To increase the speed of obtaining electronic evidence;
- To foster equal treatment of Member States in the context of direct cooperation;
- To ensure the admissibility of evidence obtained through direct cross-border cooperation;
- To increase legal certainty and reduce complexity, fragmentation and situations of conflicts of law.

[47] As noted above, pursuant to § 2702 of the U.S. Electronic Communications Privacy Act, service providers can voluntarily provide non-content data directly to foreign law enforcement upon request; they are prohibited from providing content data, except in case of an emergency.

www.parlament.gv.at

2. Possible measures

a) Production requests/orders

In order to reach these objectives, a common framework across Member States could provide a basis for and recognise the legality of the current practices of direct cooperation, i.e. providing law enforcement and judicial authorities with the competence to make non-binding production requests for cross-border access to electronic evidence, and allowing service providers to disclose electronic evidence to foreign authorities on the basis of such a production request, without passing through local law enforcement or judicial authorities.

Creating a competence for law enforcement / judicial authorities to issue cross-border production requests to service providers, and for service providers to reply to such production requests

The measure would provide a harmonised legal basis at EU level to allow law enforcement authorities to make a production request to service providers located in another Member State or in a third country, and for service providers located in the EU to reply to such requests. Production requests issued pursuant to this legal basis would not be enforceable in the country of the service provider without further action.

Another possibility that could be considered alternatively or cumulatively to the production request would be to introduce a more mandatory regime, by giving law enforcement and judicial authorities the possibility to issue and serve cross-border production orders.

Creating a competence for law enforcement / judicial authorities to issue mandatory cross-border production orders to service providers, and an obligation for service providers to reply to such requests

This measure could create a legal base for authorities in a Member State to issue and serve production orders directly to a service provider located in another Member State, without acting through another law enforcement/judicial intermediary in this other Member State, and for service providers located in the EU to reply to such requests.

www.parlament.gv.at

These measures could create a mechanism that would allow law enforcement and judicial authorities to address certain foreign service providers similarly to the way in which they address domestic providers, subject to specific conditions. Compared to the status quo on the basis of the EIO, the measures could provide for a faster procedure to obtain electronic evidence from a service provider in the EU; the comparative disadvantages of the EIO have already been sketched out above.[48]

b) Parameters for production requests/orders

For both types of measures, a number of parameters would need to be defined, including the types of data whose production can be requested or ordered: the measure could extend to all types of data or only some categories (e.g. subscriber information, traffic/metadata, content); the measure would also need to consider whether such requests should be limited to specific types of service providers (e.g. telecommunications providers and electronic communications providers) and whether exceptions are required for specific types of electronic evidence that may be subject to different regimes, such as financial records held by banks.

Furthermore, the measure would need to define the conditions under which a cross-border production request or order could be issued (and served). In particular, it would need to identify which provider can be asked to produce data on which user:

To define whether a production request/order could be used to request data relating to a particular target, the measure could rely on the material jurisdiction over a given case, or complement it with additional conditions such as the location of the target. The obligation to provide data could be limited to targets who are EU nationals or residents or extend beyond.

[48] During the expert process, Belgium presented a similar model: an obligation for companies which provide a service on EU territory (the so-called business link) to comply with EU rules and to execute national orders to provide communication data when such orders are issued by a competent authority of an EU Member State. This obligation should be enforced by a sanctions regime. It includes a possible obligation for the investigating country to demand prior or posterior agreement by other affected countries, supported by a clear definition of cases in which another country is affected by the request. BE proposes to combine two parameters: the sensitivity of the measure and the location of the target. BE considers that for the less sensitive production orders, e.g. for subscriber data, there is no need to notify another country. For more sensitive measures, such as a an order to produce content data, the key factor should be where the intrusion on the privacy of the target takes place.

www.parlament.gv.at

To define whether a production order could be issued to compel a particular service provider, possible alternative criteria (connecting factors) could be:

- the service provider has its main establishment in that Member State;
- the service provider has a significant presence,[49] such as a business link or a branch, in that Member State;
- the data controller of the service provider is located in that Member State.

The measure could be limited to service providers with a seat in the EU or extended beyond. Depending on the connecting factor chosen, the measure could provide a basis for or complement approaches under multilateral instruments, for which in particular the approach under the Council of Europe Budapest Convention on Cybercrime should be considered. Under the Budapest Convention, a guidance note was recently adopted on the use of domestic production orders for subscriber information against service providers with a business link to the country of the issuing authority (i.e. "offering its services in the territory of a Party" to the Convention).[50]

In the context of production requests, it might also be considered to allow service providers headquartered in the EU to reply to production requests from non-EU countries. In that case, the legal framework would have to comply with the EU data protection rules, which in case of a transfer of personal data by service providers to a third country are to be found in Chapter V of the General Data Protection Regulation (EU) 2016/679 (GDPR). Additional safeguards may be necessary to account for the lack of a common acquis in particular with respect to fundamental rights, including procedural rights.

In general, comprehensive guarantees and safeguards with regard to individuals' rights including judicial redress would be required. Further safeguards could also include the involvement of a judicial authority in the issuing country and could be adapted according to the sensitivity and scope of the request/order and/or the types of data requested.

[49] The degree of presence in the EU for the purposes of applying EU law varies widely across different areas of EU law, such as competition, consumer protection or data protection law. This factor requires further careful consideration.
[50] Convention Committee (T-CY) of the Council of Europe Budapest Convention on Cybercrime, "Guidance Note #10 - Production orders for subscriber information (Article 18 Budapest Convention), 1 March 2017, T-CY (2015)16.

www.parlament.gv.at

The measure would also need to determine whether the authorities of another Member State would have to be informed or involved. One of the ideas emerging from the expert consultation process is to provide for an obligation to notify the (Member) State(s) that could be affected by the investigative measure.[51] Factors to identify affected countries could e.g. be the seat of the service provider or the habitual residence of the target of the measure. The measure also would have to establish the legal consequences of the notification: it could range from a mere information to the need for the Member State notified to agree to the measure, and provide for deadlines and grounds for the Member States notified to object or refuse its agreement.

The question of user notification would also require further consideration as to whether, when, by whom and how the affected persons are notified of the measure, taking into account the need to balance both individuals' rights and the needs of the investigation, and whether there would be cost reimbursement for the provider.

The conditions, safeguards and notification requirement could be adjusted to the type of data sought, from a more lightweight procedure for subscriber data to stricter conditions for traffic or content data, bearing in mind the objective to provide added value as compared to the EIO.

Regarding the enforcement of production orders (this would not apply to production requests), a sanctions regime at EU level could be created, e.g. in the form of fines; alternatively, enforcement could be obtained via cross-border judicial cooperation.

[51] The system of notification/validation is provided by the Convention of 2000 and the Article 31 of the EIO in case of interception of telecommunication when the intercepted target is moving to or is located in another territory. Formally, law enforcement authorities continue to intercept the communication with no need of technical assistance of the State where the target is located but legally they are intercepting conversations and gathering evidence abroad.

www.parlament.gv.at

c) Analysis and comparison

Creating such an EU framework, whether based on production requests or on production orders, would provide greater legal certainty and reduce both the level of complexity and fragmentation for service providers and the conflicts of laws within the EU. A framework of this type would also contribute to transparency for individuals on the policy of direct cooperation by their service providers. It could create robust measures to ensure accountability, including through judicial redress, and improve comity among Member States through the definition of common criteria. In addition, the framework could reduce issues experienced by authorities in some Member States with the admissibility in court proceedings of electronic evidence obtained through direct cooperation. A framework of this kind would create a new dimension in cooperation in criminal matters among Member States.

www.parlament.gv.at

The measures would also allow to take into account requirements arising from the data protection framework, e.g. on documentation. Requests from law enforcement authorities to service providers regularly include personal data, e.g. a suspect's name or an IP address, in order to obtain more data of/about the suspect. The conditions for the transfer of information to recipients in third countries from a data protection perspective are provided in Chapter V of the Directive 2016/680,[52] including in particular Article 39 of the Directive, which allows competent authorities, without prejudice to any international agreement, to transfer personal data directly to recipients established in third countries in specific cases and under certain conditions. This might be applicable in case of service providers established in third countries.

When comparing the two possible types of measures – mandatory or non-mandatory – the following considerations should be taken into account:

Production requests would increase legal certainty for production requests on non-content data addressed to service providers in the U.S., which permits its service providers to directly reply to such foreign law enforcement authorities' requests. Regarding EU providers, the measure would allow them to voluntarily provide non-content data to law enforcement authorities from other Member States upon request, thereby addressing the fragmented current framework and filling a gap.

The competence for service providers to reply to requests would also provide for improved conditions for cross-border access to electronic evidence within the EU. However, the measure could only grant competence to service providers located in the EU.[53] It still depends on the willingness and commitment of service providers to cooperate, as production requests are a voluntary mechanism. The lack of enforceability would require further action through traditional channels if service providers did not cooperate with a legal request. Therefore, the considerations outlined in the December 2016 problem definition on voluntary cooperation apply *mutatis mutandis*. Creating a legal basis for a competence to initiate production requests and to allow

[52] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

[53] For production requests for non-content data addressed to service providers in the U.S., as outlined above, U.S. legislation permits its service providers to directly reply to such foreign law enforcement authorities' requests.

www.parlament.gv.at

service providers to respond to requests alone is thus not likely to fully address all identified problems and objectives.

The **production order** could achieve a number of additional objectives. Compared to a framework for voluntary cooperation, the production order would have the advantage of reliability, i.e. an obligation on service providers to respond. Service providers would have legal certainty as to their duties and their users would have clarity as to service providers' obligations.

The measures are not necessarily alternative; depending on the chosen scope, they could usefully be combined, e.g., by instituting a mandatory framework within the EU and a legal basis for production requests in situations with a connection beyond the EU.

Experts indicated that some of the practical measures set out above should be considered in parallel, to facilitate production requests and responses by service providers, e.g. by means of the establishment of central points of contact (SPOCs) at the side of law enforcement and judicial authorities.

d) Complementary procedural measures

As identified in the expert process, for situations where service providers are headquartered outside the EU, the approach could be supported by a procedural measure allowing for enforcement of the production order within the EU.

Obligation for service providers established in third countries
to designate a legal representative in the EU
for the purpose of the cooperation on the basis of production requests/orders

Service providers whose main seat is outside the EU could be required to designate **a legal representative** in an EU Member State of their choice, subject to specific conditions indicating a significant presence in one or more EU Member States.[54]

This representative would have to be empowered to receive and process a request following the solutions presented here above, which provide for a competence for issuing production request and for issuing and serving production orders within the EU.

[54] Cf. Articles 3.2 and 27.2 of the GDPR which oblige certain data controllers to designate a representative in order to facilitate the cooperation with the data protection authorities and allow for the enforcement of the EU data protection rules to the extent they apply to the foreign data controller according to the GDPR's scope of application.

www.parlament.gv.at

This measure would add a procedural facilitation to enable service and possible enforcement of requests or orders on relevant service providers. The conditions (connecting factors) allowing Member State authorities to assert jurisdiction would not be addressed in this measure, nor would the question for which types of evidence (e.g. subscriber data) the Member State authorities could assert jurisdiction. This measure would therefore need to be combined with one of the measures outlined here above to create a comprehensive framework. This solution would merely allow for the extension of those measures to service providers established in third countries.

The added value of the measure would be to turn the application of measures for production requests/orders versus service providers established outside the Union into an EU-internal process. The production request's/order's mechanism as described above could then apply, meaning that a coherent legal framework would be applied by law enforcement and judicial authorities to all service providers with a significant presence in the EU, whether or not they have their seat in the EU. Potential conflicting obligations for service providers under this obligation would have to be carefully considered and taken into account.

One of the risks of this approach would be that it could inspire third countries which do not have fundamental rights safeguards in place that can be considered comparable to ours, including in the field of data protection, to introduce a reciprocal obligation for service providers active on their territory. The potential consequences of the measure would have to be considered carefully also in the context of international trade obligations.

C. Improving the framework for direct access

The expert process also identified possible measures to streamline and harmonise the framework for direct access.

Direct access to electronic evidence can technically take place in the form of an extended search, where law enforcement authorities extend an open search of the user`s device to a remote server or data storage medium (as it may happen during a classical house search on the suspect`s premises), or in the form of a remote search when the authority`s device is used in order to access the data, often without the knowledge of the affected user(s).

www.parlament.gv.at

The use of measures providing for extended or remote access may especially be considered in situations where other forms of access (e.g. by means of cooperating with a service provider)

- are not necessary (e.g. a victim gives his/her credentials on Facebook and law enforcement authorities are able to ascertain harassing and insulting messages sent by the offender/target), or
- could undermine the investigation (e.g. in covert investigations in order to infiltrate paedophile networks), or
- are not possible or cannot be considered as feasible (e.g. when the location of the provider is unknown such as on Telegram).

Although the use of extended or remote access from an information system as an investigative measure can be strictly domestic in nature, it is becoming more likely that it may have a cross-border nature involving third countries, e.g. where the location of the infrastructure used for the processing or storage of the data or the location of the provider that enables the storage or processing of the data are in another country. Data sharding – the storage of different parts of a database across various servers that might be in different physical locations – has become a common security technique.[55] Indeed, the global nature of the internet and the growing use of cloud services make it increasingly difficult to assume that access to an information system is strictly domestic in nature.

1. Objectives

On the basis of the expert consultation process, the following objectives have been identified for improving cross-border access to electronic evidence by means of unmediated access from an information system:

- To reduce fragmentation;
- To ensure that possible effects of direct access measures on other countries are properly taken into account, based on a common understanding of relevant situations;
- Where necessary, to mitigate possible effects on other countries.

2. Possible measures

On the basis of the expert consultation process, the following measure to improve cross-border access to electronic evidence by means of unmediated access from an information system is proposed for consideration.

[55] See fn. 13 for further details.

www.parlament.gv.at

Measures for a framework for the notification of affected countries on the basis of national competence for authorities to directly access electronic evidence from an information system for the purpose of copying the information[56]

The measure would facilitate direct access to electronic evidence across borders from an information system, by means of the establishment of a harmonised framework at EU level for the notification of affected countries of the use of national investigative tools.

The framework would essentially leave it to each Member State to provide for a competence of its authorities to perform extended or remote searches.

The framework would have to include the harmonisation of certain conditions and safeguards, e.g. the mandatory involvement of a judicial authority. Depending on the national measure used (extended or a remote search), additional conditions and safeguards may also be required, such as rules on user notification.

The framework would include an obligation to notify an affected country, which could be determined by different factors such as the country where the data is located, the country where the service provider is located or where the person to whom the data relates has his or her habitual residence.

In response to the notification, the affected country could be granted the option to object to the use of the measure in specific cases.

[56] During the expert process, Germany submitted a proposal for direct access. The German proposal is also based on a system of notification/validation similar to Art. 31.EIO Directive. The criterion to determine the State affected by the investigative measures could be firstly the Member State of storage. If the investigating Member State is unable to identify the Member State of storage swiftly and with a reasonable amount of effort, the Member State of habitual residence of the person who regularly utilizes the data affected by the investigative shall be informed.

www.parlament.gv.at

The framework would apply to situations where access to electronic evidence is considered as a potential cross-border matter. This could include situations where it is clear that the evidence is located in another country, the service provider is located in another country or the habitual residence of the suspect is in another country. It should also include situations where it is unclear what the location of the evidence (loss of knowledge of location), the service provider or the habitual residence is.

The solution would leave it to Member States to provide for the competencies for their authorities to access electronic evidence without an intermediate, and would merely provide for a framework for addressing cross-border aspects of the use of the investigative measure. Considering the current differentiation of approaches of Member States, the onus to define their authorities' competences would remain at national level, while a EU measure would simply provide a framework with conditions and safeguards for the use of those measures in cross-border situations.

The use of the measure would rely on the condition of material jurisdiction of an authority as regards a certain offence. Only where an authority has the option or duty to investigate and prosecute a certain offence under its national law, it could have the competence to use direct access. Further conditions could include limiting the type of offence under investigation, or the involvement of judicial authorities for the authorisation of the measure.

The framework should provide an obligation to notify an affected country. The notification of the affected country would build on the mechanism included in Art. 31 EIO Directive. On the basis of the expert consultation process, it appears it would be most appropriate to notify the country where the person to whom the data relates has its habitual residence. In order to allow the efficient processing of notifications, the Single Points of Contact (SPOCs) mentioned above in section III.A.2 could be considered as notification contact points. Similarly, the role of national operational points of contact, as defined under the Directive on Attacks against Information Systems,[57] where not identical to the SPOC, may be considered.

[57] Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Article 13)(1) on the Exchange of information.

www.parlament.gv.at

Notifications could be for information only or provide room for objections of the receiving (Member) State as to the use of the evidence. If they were to include a possibility to object, the affected Member State could be granted the right to object within a specified timeframe.

It was raised as part of the expert consultation process that certain standards would have to be developed as regards the efforts required to be taken by the investigating authority to determine the Member State that has to be notified. It was pointed out that without operational standards, it would be difficult to establish a common EU approach on when and how a Member State affected by the use of unmediated access would have to be notified.

The measure could also include standards for user notification and would need to address the question of how to ensure effective access to measures of judicial redress in cases where the target of the measure is located abroad.

Finally, it was found as part of the expert consultation process that the possible role of third countries in relation to the use of direct access should be duly considered. This refers to all cases where it is not even possible to roughly determine the area of potentially affected third countries (e.g. "in Western Europe" or "in North America"), or where it can be determined that the location is not within the EU. It would have to be considered to what extent international instruments could be used as a basis for the application of these measures, e.g. the Council of Europe Budapest Convention on Cybercrime.[58] This being said, as part of the expert consultation process, many Member States have expressed the view that the absence of measures at international level should not prevent the establishment of rules at EU level.

The added value of the option would be to provide for a coherent framework for authorities in Member States to address situations where direct access to electronic evidence has, or may have, a cross-border aspect and thus contribute to comity. Currently, as pointed out, Member States authorities have different approaches and in some cases do not yet take into account potential cross-border aspects. This would also ensure a more coherent level of protection of the rights of targets of an investigation, e.g. with respect to user notification.

[58] As noted above, 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". See: Cybercrime Convention Committee (T-CY), Meeting report of the 16th Plenary, Strasbourg, 14 – 15 November 2016, T-CY (2016)32.

www.parlament.gv.at

The notification of an affected Member State would not only serve the purpose of the protection of the third state's sovereignty. In addition, as pointed out by practitioners as part of the expert consultation process, the notification would also prevent situations where an investigation of the authority of one Member State could interfere with an ongoing investigation of the authority of another Member State.

It should be noted that this approach could also inspire third countries to introduce a reciprocal possibility for their law enforcement authorities. A wider interpretation of the notion of "loss of knowledge of location" by third countries may lead to fundamental rights issues resulting from third country access to personal data of EU citizens without ensuring due process and legal safeguards comparable to EU standards.

D. International agreements

As part of the expert consultation process stakeholders consistently acknowledged the added value of European Union solutions, while also pointing at the limited value of regional measures in the absence of comprehensive solutions also covering other relevant countries. Indeed, the global nature of the internet and the growing use of cloud services make it increasingly important to also take account of the role of third countries.

1. Objectives

On the basis of the expert process, the objectives for improving cross-border access to electronic evidence through international agreements can be defined as follows:

- To ensure comity;
- To ensure a mutual understanding on conditions and an appropriate level of safeguards;
- To institute mutually compatible approaches and reduce conflicts of law;
- Where necessary, to mitigate possible effects on other countries

www.parlament.gv.at

2. Possible measures

Concluding multilateral or bilateral agreements to improve cross-border access to electronic evidence

Cross-border access to electronic evidence and the role of third countries could be facilitated on the basis of multilateral or bilateral agreements. These multilateral or bilateral agreements could provide for a wider scope of measures considered here above, including on production requests/orders and direct access.

The EU could seek to conclude agreements that parallel EU-internal solutions and that could institute additional safeguards with regard to individuals' rights, including judicial redress, where necessary. Safeguards could again be adapted according to the sensitivity and scope of the order and/or the types of data requested.

Regarding multilateral agreements, it should be noted that discussions are currently ongoing on the negotiation of an Additional Protocol to the Budapest Convention on Cybercrime.[59] Although the scope of the negotiations on an Additional Protocol has not yet been established, it may include provisions allowing for direct cooperation with service providers in other jurisdictions (possibly including subscriber information, preservation requests, and emergency requests), as well as provisions for a clear framework for cross-border access to information.

In the 2013 Cybersecurity Strategy of the European Union, the Budapest Convention was recognised as the main multilateral framework for the fight against cybercrime[60]. In that context, further measures to improve cross-border access to electronic evidence could be pursued as part of an Additional Protocol to the Budapest Convention.

[59] At the November 2016 meeting of the Convention Committee (T-CY) of the Council of Europe Budapest Convention on Cybercrime, the T-CY "agree[d] in principle on the need for an Additional Protocol". It was agreed to "facilitate a formal T-CY decision by June 2017 on initiating the drafting of a Protocol", for which the mandate of the T-CY Cloud Evidence Group was extended. See: Cybercrime Convention Committee (T-CY), Meeting report of the 16th Plenary, Strasbourg, 14 – 15 November 2016, T-CY (2016)32.

[60] Joint Communication of the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final

www.parlament.gv.at

Regarding bilateral solutions, the EU could aim to conclude bilateral agreements with key partners, e.g. with the U.S., to provide for production request/orders and direct access on a reciprocal base, possibly including rules for the enforcement of production orders.[61]

A multilateral solution in the framework of the Budapest Convention would have a much broader geographical scope and could possibly also include the U.S., but may not necessarily cover content data. A bilateral agreement, on the other hand, would leave the choice open as to whether to also cover content data.

In terms of drawbacks, it needs to be noted that bi- or multilateral agreements are uncertain; it could take years, if at all, to reach an agreement, be it on a multilateral agreement or on a bilateral one, and it would depend on the third countries involved.

On the other hand, these measures would have the advantage of creating more legal certainty on the basis and process for direct cooperation with private parties in third states, especially if they closely parallel choices made within the EU. Such agreements could be advantageous in terms of ensuring an adequate level of protection of fundamental rights, including data protection and to ensure enhanced transparency and accountability. It would allow for a joint definition of mutually acceptable minimum criteria and safeguards and thus help ensure comity.

V. Cross-cutting considerations

For all of the legislative measures considered here above, a number of horizontal considerations need to be taken into account. Accessing electronic evidence across borders serves the interest of effective investigations and law enforcement, and the protection of victims of crime. At the same time, when contemplating measures to facilitate access to cross-border electronic evidence, it raises 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.

[61] The U.S. and the UK have been exploring the conclusion of a bilateral agreement to permit reciprocal direct requests to service providers for access to content data, subject to specific conditions and safeguards. This agreement requires a number of legislative changes, which are pending in the U.S. A legislative proposal was submitted to U.S. Congress under the previous administration. It would require a renewed submission by the current administration to allow it to be considered by Congress.

www.parlament.gv.at

A. Territoriality

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. 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 expert process has shown the need to move away from data storage location as the key criterion.[62]

B. Procedural rights in criminal proceedings

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 the cross border nature of the measures envisaged, which would require individuals challenging 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.

[62] 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.

www.parlament.gv.at

C. Privacy and personal data protection

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. In the context of cross-border access to electronic evidence, 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.

At the same time, 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 and therefore for determining whether such interference respects the principle of proportionality. Generally speaking, access to basic subscriber information is considered as having the least impact on someone's right to privacy, whereas content data is considered as the most critical type of information in terms of what it reveals about an individual. There is no clear agreement on what constitutes metadata and where exactly it falls on this scale. Although the Commission is still assessing its impact, the December 2016 European Court of Justice's judgement in the Tele2 case appears to consider it as a rather sensitive category.

Following the expert consultation process, it appears also other non-communications related types of data have to be considered.

In that regard, it should be clearly specified what kind of electronic evidence could be provided pursuant to different types investigative measures and under which circumstances.

www.parlament.gv.at

D. Reciprocity

An important aspect to consider in case of measures that may be deemed to affect third countries is the possible reciprocal response by those third countries, which could similarly aim to access electronic evidence with a connection to the EU as defined by them, e.g. by virtue of storage location. This would be problematic where the third country does not have fundamental rights safeguards in place that can be considered comparable to the EU standard, including in the field of data protection. Legislative measures that entail reaching out to data stored in another jurisdiction, such as the system of legal representative or measures legitimising direct access, might trigger a reciprocal response by third countries. Indeed, a wider interpretation of the concept of loss of location applied by third country authorities "in reverse" may generate fundamental rights issues resulting from third country access to personal data of EU citizens.

At the same time, a number of third countries would not need to rely on reciprocal responses, as they have already put in place other approaches to ensure access to data, such as data localisation obligations or a more expansive set of investigative measures. In that light, 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.

www.parlament.gv.at