BRIEFING

Initial Appraisal of a European Commission Impact Assessment

European Parliament

European production and preservation orders and the appointment of legal representatives for gathering electronic evidence

Impact assessment (SWD(2018)118, SWD(2018)119 (summary)) accompanying a Commission proposal for a regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters (COM(2018)225) and a proposal for a directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (COM(2018)226)

This briefing provides an initial analysis of the strengths and weaknesses of the European Commission's impact assessment (IA) accompanying the above proposals, submitted on 17 April 2018 and referred to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs. The two legislative proposals are part of an initiative seeking to address obstacles in cross-border access to electronic evidence (electronically stored data) in criminal investigations. A European production order would allow a judicial authority in one Member State to request electronic evidence directly from a service provider offering services in the European Union (EU) and established or represented in another Member State, regardless of the data's location. A European preservation order would oblige a service provider to preserve specific data, which the authority could request later. Service providers offering services in the EU would be required to appoint a legal representative for the purposes of gathering electronic evidence. This initiative, which was announced in the 2017 Commission work programme, follows the communication on the European agenda on security, in which the Commission committed to review obstacles to criminal investigations into cybercrime, and its subsequent communication on a security union. The conclusions of the Justice and Home Affairs Council (JHA) in June 2016 supported this commitment and asked the Commission to make proposals in this field. In its resolution of 3 October 2017 on cybercrime the European Parliament emphasised the importance of a common European approach to criminal justice in cyberspace and called on the Commission to put forward a European legal framework for electronic evidence.[1]

Problem definition

The general **problem** is that 'some crimes cannot be effectively investigated and prosecuted in the EU because of challenges in cross-border access to electronic evidence' (IA, p. 9). The IA explains that this has negative consequences for the victims and society at large (IA, p. 21). Relevant data and service providers can be located anywhere in the world and states do not have control over data as it can swiftly cross borders (IA, p. 13). At the EU level or in the United States (US), where the headquarters of the major service providers (Google, Facebook, Microsoft, Twitter, Apple) are located, there are no mandatory retention rules and service providers have to delete data more quickly due to data minimisation requirements (IA, p. 20). The IA notes that the legal and policy framework in this field is complex, including also a data protection dimension. In cases that involve a cross-border element, authorities seek to have access to electronic evidence through i) judicial cooperation between public authorities; ii) direct cooperation between public authorities and service providers; and iii) direct access to electronic evidence by a public authority (IA, pp. 9-11).

Author: Mari Tuominen
Ex-Ante Impact Assessment Unit

PE 621.844 – July 2018

The IA identifies **three problem drivers**: (i) 'it takes too long to access e-evidence across borders under existing judicial cooperation procedures, rendering investigations and prosecutions less effective'; (ii) 'inefficiencies in public-private cooperation between service providers and public authorities hamper effective investigations and prosecutions'; and (iii) 'shortcomings in defining jurisdiction can hinder effective cross-border investigations and prosecutions' (IA, p. 22).

The IA report estimates that approximately 65 % of crime involving cross-border access to electronic evidence cannot be investigated or prosecuted effectively (IA, pp. 13, 17-18). It is estimated that there are 13 000 requests (for mutual legal assistance (MLA) or European investigation orders (EIOs)) per year between Member States (all types of data) and, in 2016, there were 1 300 requests from EU public authorities to US authorities (notably for content data, such as text, videos, images) (IA, pp. 13-14).[2] The IA explains that around 55 % of all criminal investigations included a request for cross-border access to electronic evidence and, on average, around 45 % of all requests to service providers were fulfilled in the 2013 to 2016 period (IA, pp. 14-17, 26).

The IA report notes that **judicial cooperation** between public authorities is often too slow, and administrative procedures and different legal standards may present obstacles to judicial cooperation (IA, pp. 9, 22-26, 259). Within the EU, the EIO Directive, which concerns the gathering and transfer of evidence between Member States, provides for deadlines of 120 days, but in certain cases shorter time-limits apply on account, for example, of the seriousness of the offence (IA, p. 23).[3] However, the IA considers that as the shorter deadlines are an exception, justifications should be provided in every case (IA, p. 23). Member States use MLA requests to request access to e-evidence in non-EU countries. The legal framework for MLA is complex and fragmented, involving bilateral and multilateral conventions and diverse legal systems of recipient countries. The MLA process with the US takes around 10 months (on average) (IA, p. 25). The reasons for delays relate notably to the number, quality and type of requests. The IA points out that there is also a mechanism for emergency requests under strict conditions, but 'authorities in the EU are unfamiliar with the mechanism', which the IA report does not explain further (IA, pp. 26, 84-85, 220).

Direct cooperation between public authorities and service providers, which is based on voluntary cooperation, has become the main instrument for the authorities to obtain non-content data (such as subscriber data, metadata and access logs). The number of requests to major service providers increased by 70 % in the 2013 to 2016 period (120 000 requests in 2016) (IA, pp. 14-17, 26). When it comes to direct cooperation, concerns have been voiced about the transparency of the process, the reliability and accountability of stakeholders and the reimbursement of service providers' costs. Furthermore, in most EU countries, national legislation may prevent service providers from responding to requests from authorities of another country (IA, pp. 9, 26-28, 220-225).

As regards the **direct access** channel, the location of the data may be in another country (within or outside the EU) or is not known. Member States have diverse approaches for these kind of situations, depending, for example, on whether they consider it as a domestic or a cross-border situation, and on how they proceed with remote access to data stored in another country (IA, p. 11). Member States have two mechanisms for defining their jurisdictions over electronic evidence and seeking to access it, namely domestic production orders (jurisdiction is asserted by connecting factors regarding the data, such as the storage location of the data) and direct access to data (e.g. seizure of a device, remote search of stored data). The use of different connecting factors leads to legal uncertainty and, in addition, the stakeholders, which operate in several countries, have reported conflicting national regulations and the need for a more streamlined process. There is no common view on the electronic evidence categories, which may cause uneven application of procedural safeguards and conflicts of law (IA, pp. 28-34).

In the **baseline scenario**, time delays would persist in judicial cooperation. Expected growth of electronic data would further increase the number of requests, which is likely to decrease efficiency in judicial and direct cooperation (IA, p. 77). In addition, the new data protection rules (Regulation (EU) 2016/679), are expected to restrict access, for example, to the WHOIS database, which provides

information on domain names (IA, pp. 31-32, 35, 277-279).[4] As challenges in defining jurisdiction continue, Member States may adopt new national legislation, which would increase legal fragmentation. The IA notes that the 'existing and incoming EU legislation is not likely to effectively address the challenges in cross-border access to e-evidence, in the absence of specific EU action to address those challenges in each of the channels' (IA, p. 77). In the absence of further EU action, international agreements between Member States and non-EU countries are likely to evolve in an uncoordinated way, for example, as regards bilateral agreements and in the negotiations on an additional protocol to the Council of Europe Budapest Convention on Cybercrime (launched in 2017). The IA also notes that legislation could evolve in non-EU countries (in particular the US) that are also trying to address cross-border access issues (IA, pp. 35-40, 77-79).

The IA provides a comprehensive description of the problem, which is supported by the stakeholder consultation, assessment reports, a survey targeted at the public authorities of the Member States, transparency reports by the main service providers, a review of the EU-US MLA and literature sources. The problem driver (i) regarding delays in accessing e-evidence in judicial cooperation and the problem driver (ii) regarding inefficiencies between service providers and public authorities appear to be discussed in greater detail than the problem driver (iii) concerning shortcomings in defining jurisdiction. Annex 6, which provides a more detailed analysis of the problem drivers, concerns problem drivers (i) and (ii) only. It would have benefited the analysis had there been more discussion on the complementarity between this initiative and other EU instruments in this field, such as the proposed regulation on a framework for the free flow of non-personal data, the proposed directive to empower the competition authorities to be more effective enforcers and the proposed regulation on privacy and electronic communications.

Objectives of the initiative

The **general objective** is defined as being to 'ensure effective investigation and prosecution of crimes in the EU by improving cross-border access to electronic evidence through enhanced judicial cooperation in criminal matters and an approximation of rules and procedures' (IA, p. 40). The three **specific objectives**, which address the problem drivers, are i) to 'reduce delays in cross-border access to electronic evidence'; ii) to 'ensure cross-border access to electronic evidence where it is currently missing'; and iii) to 'improve legal certainty, protection of fundamental rights, transparency and accountability' (IA, p. 41). The IA sets only one vague **operational objective**, to 'enhance operational aspects of cross-border access to criminal evidence in criminal matters' (IA, p. 110). The IA presents the operational objective after the selection of the preferred option in the monitoring and evaluation section, in line with the Better Regulation Guidelines (IA, pp. 108-110). It can be noted that the general objective refers specifically only to judicial cooperation and also mentions 'approximation of rules and procedures', whereas the problem drivers refer to issues in judicial cooperation, direct cooperation and direct access. In this respect it would perhaps have been beneficial to clarify the formulation of the general objective. According to the Better Regulation Toolbox (Tool#16), the defined objectives should be specific, measurable, achievable, realistic and time-bound (S.M.A.R.T.). The specific and operational objectives could have been formulated in a more specific and measurable manner. They are not time-bound either. The formulation of the second and third specific objectives could have been more clearly aligned with the problem drivers.

Range of options considered

To start with, the IA report explains the process of and reasons for retaining and discarding the policy measures (IA, pp. 41-42, 156-208, 238-245). The measures retained are those considered to be the most feasible, coherent, relevant and proportional to address the problem and the problem drivers. Four policy options, which are cumulative, have been developed out of the seven retained measures, in addition to the baseline. The scope of the measures covers content data and non-content data. The IA points out that different data categories may contain personal data and are 'covered by the safeguards under the EU data protection acquis' (IA, pp. 42-43). The initiative

concerns service providers regardless of where they are based and electronically stored data regardless of where it is stored. Data from real-time interception of telecommunications is excluded. The initiative concerns cross-border access to electronic evidence in the context of concrete criminal offences, which means that mass surveillance is beyond its scope. The service providers are covered in the initiative as regards the electronic communications services (e.g. SMS, over-the-top (OTT) communications services), information society services (e.g. cloud services and social networks) and internet infrastructure services (e.g. IP address providers, domain name registries) (IA, pp. 44-45).

Baseline: No further EU legislative measures to improve access to electronic evidence.

Option A (Non-legislative action): This option would aim to improve judicial cooperation in the EU (within the EIO) by using the electronic user-friendly version of the forms (EIO) and a secure online platform for exchanges of EIO/MLA requests and replies between EU competent authorities. Between the EU and the US, training for EU practitioners concerning the US system and regular contacts with relevant authorities would be organised. To enhance direct cooperation, the option would establish single points of contact, streamlined procedures and training for EU authorities on cooperation with US-based service providers (IA, pp. 79, 45-47).

Option B (Option A + international agreements): In addition to the Option A measures, this option proposes to seek to conclude international agreements, consistent with the EU approach on safeguards, in order to enhance international cooperation. The negotiations on an additional protocol to the Budapest convention may extend the existing framework to cover the establishment of a clear framework and safeguards for cross-border access and also direct cooperation with service providers in other jurisdictions. Under this option, the EU could negotiate bilateral agreements, in particular with the US, in relation to production requests or orders, direct access on a reciprocal basis and possibly rules concerning the enforcement of production orders (IA, pp. 47-50, 79).

Option C (Option B + direct cooperation legislation): Building on Option B, this option comprises a European production order (EPO) and access to databases (WHOIS). The EPO could be addressed directly to a service provider in another country irrespective of where the service provider is based (in or outside the EU) or where the data is stored. As an auxiliary measure to the EPO, an order to preserve the data could be included in the initiative. The EPO would oblige the service provider concerned to cooperate within the deadlines (normal or urgent cases). In the event of non-compliance this option provides for sanctions to be imposed and executed within the EU through mutual recognition mechanisms and with non-EU countries through applicable international agreements. This option also provides for a conflict of law clause, which would protect service providers in cases of conflicting obligations arising from the national law of non-EU countries, and that could address reciprocity issues. The EPO would comprise safeguards, such as the principles of necessity and proportionality, the procedural rights of accused and suspected persons, user notification, legal remedies and the requirement that an EPO must be issued or validated by a judicial authority. Service providers operating in the EU would be obliged to designate a legal representative for cooperation with the public authorities of the requesting Member State. While the new data protection Regulation (EU) 2016/679) restricts the information available, this option would retain access to databases such as WHOIS for public authorities (IA, pp. 50-67, 79-81).

Option D (preferred option) (Option C + direct access legislation): In addition to Option C measures, this option would, in particular, allow public authorities to access data directly, at least that regarding serious crimes, when there is no certainty that the data is stored in the same Member State. A set of conditions for issuing a judicial order (permit for direct access) would be defined. This option comprises direct access with the agreement of the data subject (i.e. the victim or witness), an extended search (ongoing search), and a remote search (using lawfully obtained user credentials). Safeguards would be applied, such as the requirement that a judicial authority validate direct access, the principles of necessity and proportionality, procedural rights of accused and suspected persons, user notification and legal remedies (IA, pp. 67-71).

The options are clearly linked to the objectives and the problem definition and they derive from the stakeholder consultation. However, the views of the stakeholders are not clearly presented for each option. The range of options seems to be sufficiently broad, and include a non-legislative option, as required in the Better Regulation Guidelines. The preferred option is Option D.

Scope of the impact assessment

The IA explains that a qualitative assessment was at first carried out in terms of the social, economic and fundamental rights impacts of all measures, after which a qualitative assessment was carried out for all options. No significant environmental impacts are expected (IA, pp. 82-97). The options were qualitatively assessed against the criteria of effectiveness, efficiency, competitiveness, fundamental rights, impact on international relations and achieving the specific objectives. Proportionality is also discussed. The IA notes the limited quantification of costs and benefits owing to a lack of data. The international agreement measures have not been quantified as it is uncertain what the outcome of the negotiations concerned would be (IA, pp. 97-106). The IA report provides a detailed comparative assessment of all options in Annex 4 (IA, pp. 156-208). The preferred Option D would, according to the IA report, improve public authorities' capacity to investigate and prosecute crimes and contribute to legal certainty and transparency in direct cooperation with service providers. The conflicts of law clause in the EPO and international solutions would also 'significantly reduce the risk of reciprocal responses from non-EU countries' (IA, p. 107). Furthermore, expected impacts include cost savings and a reduced burden for authorities. The IA also openly explains the weaknesses of the preferred option, namely that in the judicial cooperation channel in the EU, the current 120 day-deadline would remain (EIO). Furthermore, the EPO would not allow EU authorities to obtain content data from US providers on account of conflicts with US law, concluding a bilateral agreement would take a long time and, therefore, MLA channels would be used. Furthermore, according to the IA the 'measures to facilitate direct cooperation may have a considerable impact on fundamental rights' as the public authorities would have access to data, which is not publicly available and that is often personal data. The IA explains that the use of sufficient safeguards and minimum conditions in the measures would ensure that fundamental rights and data protection rules were upheld (IA, p. 107). The IA report explains that experts in fundamental rights and data protection from the Member States and the European Data Protection Supervisor assessed the fundamental rights aspects in the consultation process, and that the 'safeguards that are part of the legislative measures are the result of this assessment' (IA, p. 92).[5]

Subsidiarity / proportionality

The legal bases are Articles 82(1), 82(2), 53 and 62 of the Treaty on the Functioning of the European Union (TFEU). Article 82(1) concerning judicial cooperation would, according to the IA, cover legislation on direct cooperation between authorities and service providers. The IA considers that 'this would introduce a new dimension in mutual recognition, beyond the traditional judicial cooperation' (IA, p. 37). Cross-border cooperation is often required to access electronic evidence in criminal investigations and therefore action at EU level would be necessary to address the problems identified. According to the IA report, international rules are insufficient to tackle the problems, whereas a combination of international and EU instruments would have a more effective impact (IA, pp. 39-40). The IA notes that the preferred option would not go beyond what is necessary to achieve the defined objectives, given also that conditions and safeguards are included in the measures, in particular in view of data protection (IA, p. 108). The deadlines for the subsidiarity check for national parliaments are 13 September 2018 (for the regulation proposal) and 10 September 2018 (for the directive proposal). No reasoned opinions had been submitted at the time of writing.

Budgetary or public finance implications

The initiative would not have an impact on the EU budget. The preferred option would entail administrative costs for public authorities relating to transposition (one-off costs are estimated at

€3.3 million) and enforcement as well as compliance costs for service providers (one-off costs of €1.7 million). The IA estimates that national authorities and service providers would benefit from streamlining and a clearer legal framework. Moreover, an expected shift from the judicial cooperation to the direct cooperation channel would decrease the number of requests that national authorities have to process. The annual savings are estimated at over €7.1 million for public authorities and over €4.3 million for service providers (IA, pp. 98-101 and Annex 4, pp. 156-208).

SME test / Competitiveness

The IA provides an SME test, including an assessment of mitigating measures. The IA explains that up to 90 % of the cross-border requests concerning non-content data are addressed to the major service providers and only a small number of requests concern SMEs. In the consultation process, SMEs raised concerns regarding administrative burden and compliance costs, while stressing the need for legal clarity. The EPO would increase administrative costs for SMEs (EU and non-EU), when receiving requests from other countries. The obligation to nominate a legal representative would generate costs, which may be a burden especially for those SMEs that offer services in the Union but are not established in the EU. The IA notes that the legal representative could be shared by several SMEs and also points out that the nomination obligation will not apply in case of only occasional data processing in the EU. On the other hand, the IA notes that legal certainty and standardisation of procedures would reduce the administrative burden and favour competitiveness, which would have a positive impact on SMEs (IA, pp. 45, 91, 167-168, and Annex 13, pp. 280-282).

Relations with third countries

Bilateral and multilateral agreements are among the measures in the preferred option as international solutions are needed, for example, to address the risk of issues concerning conflicts of law and reciprocal responses and to impose on and execute sanctions against service providers in cases of non-compliance with the EPO request. As the main service providers are headquartered in the US, the evolution of legislation in the US is relevant to EU-US cooperation. The IA stresses the importance of having a coordinated EU position for international agreements, such as for the negotiations on the additional protocol to the Budapest Convention on Cybercrime (IA, p. 49).

Simplification and other regulatory implications

The legal environment is evolving in this field as several EU instruments are under revision. The IA explains how this initiative would relate to the EIO. It should be noted that there is not yet much experience of the EIO, given that it has only been in application since May 2017. The IA describes several proposals for EU legislation that have links to the initiative, but it would have been useful to have had further information on the complementarity between this initiative and proposed EU instruments, for example, concerning privacy and electronic communications or the free flow of non-personal data (IA, pp. 247-248).

Quality of data, research and analysis

Overall, the data provide a sound source of information. The preparation of the IA has been supported by recent reports, studies, literature and a stakeholder consultation, in particular the expert consultation process between July 2016 and October 2017.[6] In the Commission, a joint HOME/JUST taskforce and an inter-service group have been working on the initiative. The IA provides a qualitative and quantitative assessment. The Commission is open regarding the limitations of the quantification of costs and benefits owing to a lack of data. The IA explains the methodology, assumptions and calculations used in Annexes 3 and 4 (pp. 147-208). According to the IA, links to the sources have been included 'whenever possible' (IA, p. 116).

Stakeholder consultation

The extensive stakeholder consultation process is explained in the IA, as required by the Better Regulation Guidelines (Annex 2, pp. 117-146). An expert level consultation was organised between

July 2016 and October 2017, involving, for example, service providers, industry associations, civil society organisations, practitioners, data protection authorities, the European Data Protection Supervisor, Europol and several EU-level networks (IA, pp. 137-139). An open public consultation took place over 12 weeks (between 4 August 2017 and 27 October 2017) and resulted in 82 responses (22 individuals, 60 practitioners). It gathered information on the weaknesses of the current legislation and possible solutions. The inception impact assessment (between 4 August 2017 and 31 August 2017) triggered 10 feedback responses. Three targeted surveys of public authorities were carried out concerning current practices, the scale of the problem and costs and benefits (between 26 July 2016 and 8 November 2017). One targeted survey on costs and benefits was addressed to service providers within and outside the EU (between 25 October 2017 and 8 November 2017). The IA also refers to bilateral meetings for example with service providers, public authorities and NGOs (between April 2016 and November 2017). Stakeholders had mixed views on the EPO as public authorities had more positive views than service providers on it. Service providers and civil society respondents stressed the need for a clear framework with sufficient safeguards. Non-legislative measures were widely supported and international agreements were 'cited as good options by a range of stakeholders'. Stakeholders' views are mentioned in a rather general way ('a range of stakeholders', 'service providers', civil society', authorities', 'expert feedback') (IA, pp. 84-90) throughout the report.

Monitoring and evaluation

The IA report presents a monitoring table with indicators, data sources and the general, specific and operational objectives (Table 13, p. 110). According to the IA, the Commission should elaborate an assessment report two years after the deadline for transposition and an evaluation report five years after the deadline for implementing the legislative act, including also a public consultation and possibly a survey of stakeholders. The existing data sources would be used, but in case of lack of data, Member States are requested to systematically collect it, for example on the time delays and percentage of requests fulfilled (IA, pp. 108-110 and Table 13, p. 110).

Commission Regulatory Scrutiny Board (RSB)

The RSB issued a positive opinion on 15 December 2017 with a recommendation to improve the IA report on the main following points: i) further discussion of fundamental rights in relation to the proposed measures and appropriate safeguards; ii) description of how the views of stakeholders and Member States have been taken into account; iii) reference to measures for improving cooperation among judicial authorities and with service providers and an explanation as to how the proposed measures complement other initiatives. As required by the Better Regulation Guidelines, the IA explains in Annex 1 how the remarks of the RSB have been addressed (IA, pp. 113-115). On the whole, efforts have been made to address the RSB's remarks. Fundamental rights are discussed under each option and safeguards are explained. It would nevertheless have been useful to have had more specific indications of the various stakeholders' views under each option and further description of the complementarity between this initiative and other proposed EU legislation.

Consistency between the Commission's legislative proposals and the IA

The proposed directive on the appointment of legal representatives appears to be consistent with the recommendations of the IA. However, the proposed regulation appears to follow the IA's preferred Option D only in part. The Commission does not propose legislation for measures on direct access and access to databases, 'but will reflect further on the best way forward on these two issues' (Explanatory Memorandum of the regulation proposal, p. 9). In addition, in relation to transactional data or content data, the proposal would limit use of the EPO to cases of more serious crime only. An EPO may be issued if a similar order would be available for the same criminal offence in a comparable domestic situation in the issuing state.

Conclusions

The IA provides a comprehensive description of the problem, supported by an extensive stakeholder consultation, reports and literature. The options are clearly linked to the objectives and the problem definition. More attention appears to be given to problem drivers (i) regarding delays to access e-evidence in judicial cooperation and (ii) regarding inefficiencies between service providers and public authorities than to problem driver (iii) concerning shortcomings in defining jurisdiction. The analysis would have benefited from a more detailed analysis of the consistency and complementary between this initiative and other proposed EU legislation. Furthermore, a breakdown of stakeholders' views under the various options would have been useful. Finally, it should be noted that the proposed regulation does not entirely follow the IA in that it does not include the legislative measures on direct access and access to databases envisaged by the IA's preferred option. In addition, the proposal includes additional conditions for issuing an EPO.

ENDNOTES

[1] See European Parliament resolution of 3 October 2017 on the fight against cybercrime.

[2] Content data: 'The substance of stored information, such as text, voice, videos, images, and sound'. Non-content data: subscriber data, metadata, access logs, transaction logs. Subscriber data: 'Information allowing to identify a natural person or legal entity using services provided by relevant service providers'. Metadata: 'Data processed for the purposes of transmitting, distributing or exchanging electronic communications or other content through a network'. Access logs: 'Record the time and date an individual has accessed a service and the IP address from which the service was accessed'. Transaction logs: 'Identify products or services an individual has obtained from a provider or a third party' (IA, pp. 3-4).

[3] Directive 2014/41/EU (the EIO Directive) has been in application since May 2017. Ireland and Denmark do not participate in the EIO Directive and therefore the EIO deadlines do not apply in these countries (IA, pp. 23-24).

[4] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); came into force on 25 May 2018.

[5] At the time of writing, the European Data Protection Supervisor has not yet issued an opinion on the legislative proposals. See the statement by the Article 29 Data Protection Working Party (replaced by the European Data Protection Board (EDPB) as of 25 May 2018).

[6] Final report of the seventh round of mutual evaluations on 'The practical implementation and operation of the European policies on prevention and combating cybercrime' (GENVAL Report), ST 9986/17; T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime (2-3 December 2014); Council of Europe Budapest Convention on Cybercrime, T-CY, Criminal justice access to data in the cloud: Cooperation with foreign service providers, 3 May 2016 (provisional); Transparency reports 2016 by Google, Facebook, Microsoft, Twitter and Apple; Five year review carried out in 2016 of the EU-US MLA agreement; Europol: Internet Organised Crime Assessment (i-OCTA) 2017.

This briefing, prepared for the Committee on Civil Liberties, Justice and Home Affairs, analyses whether the principal criteria laid down in the Commission's Better Regulation Guidelines, as well as additional factors identified by Parliament in its Impact Assessment Handbook, appear to be met by the IA. It does not attempt to deal with the substance of the proposal.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)