Cross-border Access to E-Evidence: Framing the Evidence

Fuster, Gloria González; Vazquez Maymir, Sergi

Publication date:
2020

CEPS Paper in LIBERTY and SECURITY in Europe

Cross-border Access to E-Evidence: Framing the Evidence

Gloria González Fuster and Sergi Vázquez Maymir

No. 2020-02, February 2020

Abstract

This paper aims at situating the policy discourse accompanying current European Union (EU) initiatives on facilitating access by public authorities to data held by private companies, including in scenarios regarded as crossing jurisdictional borders. More concretely, it contextualises these initiatives in light of the absence of publicly available statistical information on some of the issues which are at the very core of these matters.

Firstly, the paper presents the three main current developments, that is, the proposed 'E-evidence package', the negotiation of an EU-United States (US) agreement facilitating access to e-evidence for the purpose of judicial cooperation in criminal matters, and the participation of the EU in the negotiations in the Council of Europe on a second additional protocol to the Cybercrime Convention, analysing some of the recurrent messages associated with defending the necessity of all these different measures. The Brief then reviews some of the information upon which are being constructed arguments used to purport the need for these developments, by granting particular attention to the Impact Assessment that accompanied the publication of the 'E-evidence package'. Finally, it suggests that the absence of statistical data might have implications for the assessment of the proportionality of eventual legislative measures.

This paper has been prepared in the context of the JUD-IT (*Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU: Ensuring Efficient Cross-Border Cooperation and Mutual Trust*) Project, with financial support from the Justice Programme of the European Union (JUST-AG-2016-01). The opinions expressed in this report are attributable solely to the authors in a personal capacity and not to any institution with which they are associated, nor can they be taken in any way to reflect the views of the European Commission.

Gloria González Fuster is a Research Professor and Co-Director of the Law, Science, Technology & Society Research Group at the Vrije Universiteit Brussel.. Sergi Vázquez Maymir is a Doctoral Researcher and member of the Fundamental Rights Research Centre at Vrije Universiteit Brussel.

978-94-6138-763-9

Contents

List of Figures and Tables

List of abbreviations

EIO	European Investigation Order
EPO	European Production Order
EU	European Union
MLAT	Mutual Legal Assistance Treaty
US	United States

Introduction

The European Union (EU) is currently engaged in a number of developments aimed at facilitating the access by public authorities to personal data held by private companies, for the purpose of serving as evidence in criminal proceedings. In line with these developments, the access to data should ultimately be rendered possible, whenever necessary, regardless of the eventual crossing of jurisdictional borders – be it borders between different Member States, or between the EU and certain third countries. Current developments are indeed based on the general premise that crime does not stop at borders between countries, and that, therefore, shall be facilitated the access by public authorities to any data useful in the context of criminal proceedings, also across borders.

This Policy Brief provides a descriptive overview of the instruments on the table, giving particular attention to the question of how their necessity is being presented, and the publicly available evidence used to support such necessity. It first introduces the instruments, pointing out some of their interconnections, but also their disparate legal implications, as well as commenting the argumentation surrounding them. The paper later moves to discussing more in detail the Impact Assessment that accompanied the publication of the 'E-evidence package' made public by the European Commission in 2018.

1. Three initiatives and a leitmotif

Ongoing policy discussions at EU level in relation to cross-border access to evidence concern mainly three elements. First, there is the so-called 'E-evidence package', referring to both a proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters,[1] and a proposal for a Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.[2] These two texts were made public by the European Commission in April of 2018; the Council reached a position on the proposed Regulation in December 2018,[3] and on the proposed Directive in March 2019.[4]

These proposals are intended, in particular, to facilitate access to e-evidence by enabling judicial orders emanating from one Member State to be addressed directly to service providers based in another Member State. They also aim, *inter alia,* at avoiding fragmentation in the EU,

[1] European Commission (2018), *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 final, Strasbourg, 17.4.2018.

[2] European Commission (2018), *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 final, Strasbourg, 17.4.2018.

[3] And supplemented by the respective annexes to that proposal as agreed by the Council (Justice and Home Affairs) at its meeting on 6 June 2019: Council of the EU (2019), *General approach to Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters*, 10206/19, 11.6.2019.

[4] Council of the EU (2019), *General approach to 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,* 6946/19, Brussels, 28.2.2019, adopted on 8 March 2019.

which could be created by disparate national requirements imposed on service providers, including non-EU providers, in relation to measures concerning requests for data – for instance, referring to the need to have a legal representative within the territory of the Member State.

To this purpose, the proposed Directive regulates the appointment of service providers' legal representatives, entrusted with receive and responding to orders requesting data, for non-EU service providers providing services within the EU: shall be obliged to designate a legal representative all service providers that offer services in the EU, meaning in one or more Member States. The mere accessibility of an online interface, taken in isolation, shall not be a sufficient condition to trigger this obligation. What would matter are the existence of a substantial connection with one or more Member States, or specific factual criteria such as a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States.

Second, the Council of the EU mandated the European Commission to negotiate on behalf of EU with a view to concluding an agreement between the EU and the US on cross-border access by judicial authorities in criminal proceedings to electronic evidence held by a service provider,[5] based on a Recommendation put forward by the European Commission in February 2019.[6] This Agreement should notably reduce the problems of conflicts of law potentially affecting US service providers which might need to comply with future E-evidence rules, in particular in the cases where they might receive their legal representative in the EU, a data request in the form of a European Production Order (EPO). In doing so, it would be instrumental for the effectiveness of EPOs, as the largest service providers are headquartered in the US.[7]

Third, the Council also mandated the European Commission to participate in the negotiations in the Council of Europe on a Second Additional Protocol to the Cybercrime Convention (known as the Budapest Convention), again based on a Recommendation put forward by the Commission in February 2019.[8] This Second Additional Protocol, which is under discussion at the Council of Europe since 2017, would lay down rules allowing for direct requests for data to be sent to service providers in other states parties to the Convention. Currently, 63 countries are party this Convention: 26 are EU Member States and thus share, notably, the same data protection standards, while the majority are not. Countries include the US, as well as Turkey,

[5] Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Brussels, 21.5.2019.

[6] European Commission (2019), *Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, COM(2019) 70 final, Brussels, 5.2.2019.

[7] In this sense: European Data Protection Supervisor (EDPS) (2019), *Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence,* Opinion 2/2019, 2.4.2019, p. 6.

[8] European Commission (2019), *Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185),* COM(2019) 71 final, Brussels, 5.2.2019.

Russia, Canada, Israel, and Nigeria, to name a few examples illustrating its broad geographical scope.

These three elements currently on the table of EU decision-makers are, as already hinted, interconnected at a number of levels. They all mirror a parallel concern with tackling a perceived inadequacy of existing legal channels for public authorities to obtain access to data in the hands of service providers, these data being really at the centre of policy attention.

2. Three different sets of legal implications

The three described, elements, however, do also have different legal implications, especially in terms of impact on EU fundamental rights. They would indeed have different, incremental effects on accessibility of personal data processed under EU law.

The E-evidence package targets, as such, the access by public authorities to data in the hands of service providers operating in the EU. In this context, the 'cross-border' dimension of this package refers first and foremost to the fact that the authority and the service provider might not be based in the same Member State: the request might thus 'cross a border' that until now prototypically requires going through a contact with another public authority on the other side of the border. In doing so, what this package does is multiply the possibilities for service providers to be directly contacted by a public authority seeking access to the data they process. Service providers could be potentially directly addressed by any competent authority from any Member State, and not only, for instance, the one where they are based, or where they predominantly deliver services, or where they store their data.

The E-evidence package's implications, however, go actually beyond that, as the rules under discussion would generally oblige certain third-country service providers to designate a legal representative in the EU, who would have to fulfil request for data presented by competent authorities of EU Member States. This means that data that could arguably be 'at the other side' of the jurisdictional border would be in way re-located under the jurisdictional reach of EU competent authorities.

The possible future EU-US Agreement should, according to the Council, *"[a]ddress conflicts of law and set common rules for orders for obtaining electronic evidence, in the form of content and non-content data, from a judicial authority in one contracting party, addressed to a service provider that is subject to the law of the other contracting party*". [9] In line with the mandate to negotiate an EU-US Agreement, the instrument *"should create reciprocal rights and obligations of the parties*".[10]

[9] Council of the EU (2019), *Addendum to the Recommendation for a Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters - adoption*, Brussels, 27.5.2019, p. 3.
[10] Ibid., p. 4.

This reciprocity principle is of the greatest importance, as it implies that increased, faster access to data by European public authorities is to be obtained only on the condition that an 'equivalent' access to data held by EU service providers is guaranteed to US public authorities. In doing so, this Agreement would thus in a way move data from under EU law to the reach of US authorities, redrawing the boundaries of their reach.

The future EU-US Agreement would, in the bilateral relations between the EU and the US, take precedence over the Council of Europe Convention on Cybercrime and any agreement or arrangement reached in the negotiations of the Second Additional Protocol to the Council of Europe Convention on Cybercrime, in so far as the provisions of the latter agreement or arrangement cover issues dealt with by the EU-US Agreement.[11]

The implications of the discussed Second Additional Protocol to the Council of Europe Convention on Cybercrime would be rather global in nature, potentially allowing EU competent authorities to 'cross' a significant number of borders in their quest for data, while, at the same time, putting data protected under EU law within the reach of a significant number of third countries.

3. More, faster, smoother

The need for new instruments in the area of 'cross-border' access to data is typically connected in EU policy documents to a variety of arguments, among which might be described three main groups: those concerned with the need to obtain access to certain data presumably inaccessible (that is, to reach *more* data), those related to accelerating the process of accessing such data (thus, to reach them *faster*), and those generally linked with facilitating and reducing any possible obstacles to the whole endeavour (to reach the data *in a less cumbersome manner*).

It is worth being underlined that discussions have regularly centred on granting increased, quicker, and more direct access to data in relation to all types of crimes, as opposed to regulating merely criminal proceedings related to certain categories of crimes such as, for instance, 'cybercrimes'. Documents typically stress that e-evidence is increasingly of significance in all criminal proceedings – at least to the extent that there is e-evidence related to the proceedings at stake. As somehow tautologically stated by the Council: "*The collection, analysis and usage of e-evidence is increasingly relevant in criminal proceedings, not only in relation to cybercrime, but also in relation to any other offence that may involve e-evidence*".[12]

[11] Ibid., p. 5.

[12] Council of the EU (2017), *Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime"*, ST 12711 2017 INIT, Brussels, 2.10.2017, p. 45.

3.1 More

The idea that nowadays some data remains inappropriately out of reach for EU competent authorities to access them and allow for their use in criminal proceedings concerns mainly certain categories of data, and, specifically, 'content data', in the sense of data related to the content of electronic communications.

More specifically, this limitation crucially concerns US service provides, which are currently allowed by US law to disclose some data to public authorities of foreign countries, but not content data. The legal situation of requests for content data submitted to US services providers might be changed under the US Clarifying Lawful Overseas Use of Data (CLOUD) Act,[13] if qualifying foreign governments would conclude an executive agreement with the US to allow for the fulfilment of these requests when emanating from certain foreign countries. It is in the context of this specific possibility that needs to be placed the EU-US Agreement under negotiation, which would thus not only be instrumental for US service providers to be able to fulfil their obligations under the E-evidence package, but also instrumental for them to translate into reality the possibilities opened up by the CLOUD Act.

3.2 Faster

The presumably problematic slowness of existing procedures has been decried in numerous occasions: "*the current MLA procedures need to be faster*", stated, for instance, the Council.[14] In some occasions it is unclear exactly to what this comparative refers to: procedures might need to be faster in the future than they are in the present, but also, perhaps, faster than data being moved by criminals.

The Impact Assessment accompanying the E-evidence package noted that in the cases in which electronic evidence is available only on private infrastructures located outside a country, or owned by service providers established outside of such country, or both, "*traditional mechanisms for cooperation between authorities are slow compared to the fast pace at which data can be moved, changed or deleted*"[15]. In these instances, speeding up the access to data seems to aim, ultimately, at guaranteeing that the access is faster than the data, which appears to be, somehow, escaping from attempts to access it. Because data moves fast away from public authorities, public authorities would need to be quicker than such movement: "*authorities face a race against time to obtain data for their investigation"*, as the European Data Protection Supervisor (EDPS) eloquently wrote.[16]

The fundamental question in relation to this is, ultimately, whether the speeding up shall be attempted by improving the performance of existing mechanisms, or by proposing alternative channels for obtaining access.

[13] Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943).
[14] Council of the EU (2017), op. cit., p. 48.
[15] Ibid., p. 5.
[16] EDPS (2019), op. cit., p. 3.

3.3 Smoother

Rendering the whole process of accessing data held by private companies less cumbersome for public authorities has been a recurrent concern among EU institutions discussing these questions. Sometimes, this facilitation of access goes hand in hand with a call to re-imagine existing access paradigms governing international cooperation, which are based in the notion of judicial cooperation. Judicial cooperation is at the heart of existing mechanisms such as the European Investigation Order,[17] the 2000 Mutual Legal Assistance Convention,[18] or the 2013 EU-US Agreement on Mutual Legal Assistance.[19]

"*Cyber criminality requires competent judicial authorities to rethink the way they cooperate within their jurisdiction and applicable law to ensure swifter cross-border access to evidence and information*", stated the European Commission in 2015.[20] Already then, the Commission identified as a point for future action a review of the "*obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information*".[21]

Progressively, this re-thinking of cooperation has been shaped along the lines of allowing public authorities to request directly to private companies access to data they hold, even when the issuance of such a request, or the granting of access to the data, might appear to cross jurisdictional border. This, as a matter of fact, goes beyond a re-thinking of the way in which judicial authorities cooperate between them, towards a focus on letting public authorities work directly with private actors.

The possibility for public authorities to request the data directly to private companies, also in cross-border scenarios, can be described as 'unmediated access',[22] in the sense that it does not rely on the involvement of an authority mediating the submitted request on the other side of the border. The European Commission appears to favour the label of 'direct cooperation', which would be different from 'judicial cooperation' but also from 'direct access'. In this

[17] 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, 1.5.2014, pp. 1-36.
[18] 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, OJ C 197, 12.7.2000, p. 1 and its Protocol, OJ C 326, 21.11.2001, p. 1-2.
[19] Agreement of 25 June 2003 on mutual legal assistance between the European Union and the United States of America, OJ L 181, 19.7.2003, pp. 34-42.
[20] European Commission (2015), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions*: *The European Agenda on Security*, COM(2015) 185 final, Strasbourg, 28.4.2015, p. 20.
[21] Idem.
[22] Sergio Carrera, Gloria González Fuster, Elspeth Guild, and Valsamis Mitsilegas (2015*), Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights,* CEPS, Brussels, p. 9.

tripartite division, 'direct access' would take place when a public authority actively retrieves data from a private company without the latter being requested to cooperate.[23]

4. The evidence behind E-Evidence

In 2017, following a round of mutual evaluations on the prevention and combating cybercrime, the Council recommended that the EU and its Member States consider the development of an EU framework on law enforcement access to data held by service providers, which *"should regulate the relations between LEA and ISPs, with clear rules and duties".*[24] That round of mutual evaluations did gather a considerable of information on national practices related to cybercrime, as collected by punctual visits of teams of three national experts in the field.[25]

A more specific discussion of information specifically related to e-evidence can be found in the Impact Assessment that accompanied the publication of the E-evidence package by the European Commission in April 2018. This Impact Assessment draws on a variety of sources, including information gathered via the consultation activities that were put in place by the European Commission during the preparation of the package. These consultation activities notably encompassed meetings, participation to conferences, an open public consultation, and a series of 'targeted surveys': a total of three surveys of public authorities in Member States, one on current practices, a second one on "*the size of the problem*", and a third one on costs and benefits associated with different options; plus another survey, also on costs and benefits associated with the different options, targeting service providers.[26]

4.1 Getting to know the unknown

The Impact Assessment openly concedes that there are important limitations in terms of available information on the issue at stake. It notes that "[i]*t is not possible to determine exactly the number of crimes that cannot be effectively investigated and prosecuted in the EU because of challenges in cross-border access to electronic evidence"*, explaining that "[d]*ata at this level of detail is not collected by public authorities*".[27] There might be some irony in the fact that these public authorities that do not deem the collection data on such matters necessary or appropriate correspond, at least partially, to the very same authorities that are eager to

[23] Or, as the Impact Assessment accompanying the E-evidence package states "*without the help of an intermediary*" (European Commission, Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and 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, SWD/2018/118 final, Brussels, 17.4.2018, hereafter 'the Impact Assessment', p. 11). In practice, this notion of "help" might be difficult to assess, as for instance a known vulnerability could also be regarded as "help".

[24] Council of the EU (2017), op. cit., p. 50.

[25] National reports on the evaluations are available here: https://www.coe.int/en/web/octopus/blog/-/blogs/genval-evalutation-reports-on-cybercrime/.

[26] Impact Assessment, p. 118.

[27] Ibid., p. 13.

highlight the need for them to obtain access to more data, faster, in a less cumbersome manner, including across the globe.

The document offers nevertheless some estimations, notably regarding the number of yearly judicial cooperation requests, based on available data on the European Arrest Warrant and from the European Judicial Network ("*it can be estimated that there are around 13,000 MLA/EIO requests per year on e-evidence between Member States*"), and the figures collected during the 2016 EU-US MLA Review exercise ("*it can be estimated that the outgoing requests for e-evidence by EU public authorities to the US authorities amount to approximately 1300 per year*").

4.1.1 Ten months it shall be

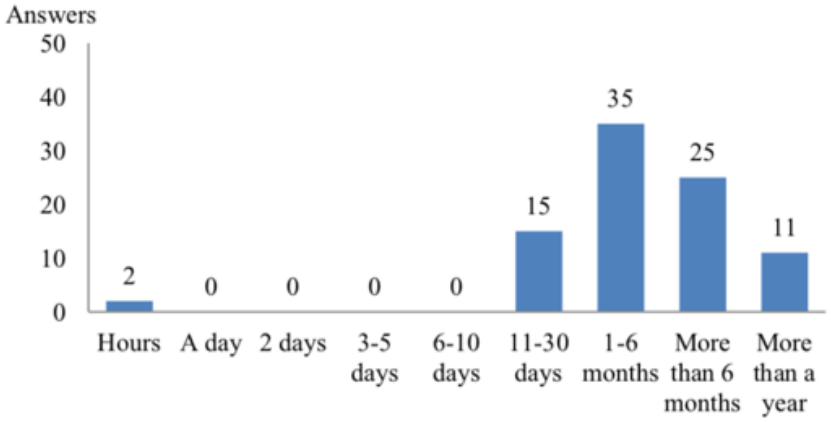
Some of the sources cited in the Impact Assessment are peculiar. In this sense, it proclaims that "[t]*he MLAT process with the US takes an average of 10 months*", referring in a footnote to a blog post by an academic, dated from 2016.[28] In such blog post, it is indeed stated that, in relation to UK requests to data sent to the US, *"[t]his process takes an average of 10 months*", an assertion provided without a specific reference as such; previously, the post does refer to another post, which similarly refers to "*a process that takes an average of 10 months*", again without any concrete reference, and to another blog post, from 2015,[29] which does directly mention the source of such assertion – a 2013 report which stated that *"[r]equests appear to average approximately 10 months to fulfill, with some requests taking considerably longer*".[30] Such 2013 put forward that statement without any further clarification as to how this exact figure had been calculated, and – again ironically, perhaps- did so in an introductory paragraph that presented a series of recommendations on how to actually improve mutual legal assistance mechanisms, as opposed to dismissing them, or getting rid of them, and this in order to "*demonstrate the US commitment to a well-functioning Internet that meets the goals of the international community*".[31]

This recurrent idea of a duration of 10 months is not explicitly contrasted with insights revealed through other sources used by the European Commission. The figure below, for instance, is presented in the Impact Assessment and would suggest that for the majority of surveyed contacts requests for content data to third countries would believe take an average time of up to 6 months.

[28] Jennifer Daskal (2016), "A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right", *Just Security,* February 2016, https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/.
[29] David Kris (2015), "Preliminary Thoughts on Cross-Border Data Requests", *Lawfare*, September 28, 2015, https://www.lawfareblog.com/preliminary-thoughts-cross-border-data-requests.
[30] United States President's Review Group on Intelligence and Communications Technologies, Richard Alan Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter P. Swire (2013), *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies,* December 2013, p. 227.
[31] Idem.

Figure 1. Table from Impact Assessment, p. 263

Figure 11: the time it takes to receive a response to a request for content data to service providers via public authorities in non-EU countries



4.1.2 The persistent opacity of transparency reports

The European Commission asserts it estimated "*the magnitude of the problem*" which the E-evidence package tries to solve primarily using two main sources of information: the survey analysed in the following section, and so-called 'transparency reports' from the main service providers, that is, Facebook, Google, Microsoft, Twitter and Apple.[32] According to what are apparently the European Commission's own calculations, the market share of these companies would allow to 'estimate' "*that up to 90% of current cross-border requests for non-content data are sent to these five providers*".[33]

The Impact Assessment notes these transparency reports suffer from important limitations. For instance, they do not distinguish whether reported requests came directly from the Member State in which it originated, or from an authority which mediated such request, and concern "*mostly*" requests for non-content data.[34]

4.2 A survey which proved (also) other matters

A particularly interesting survey among those conducted by the European Commission in preparation for the E-evidence package is the survey of public authorities in Member States on "*the size of the problem*", aiming at collecting both quantitative and qualitative information on the subject. This enquiry illustrates many of the difficulties in quantifying "*the size of the problem*" with any degree of precision, even if its results were, *de facto*, eventually used by the

[32] Impact Assessment, p. 14.
[33] Idem.
[34] Idem.

European Commission to put forward a set of relatively straightforward, factual-sounding assertions in the Impact Assessment.[35]

The survey was carried out in October 2017 through an online questionnaire made available to representatives of public authorities. It is probably better understood as primarily a consultation tool, contributing to the exploration of experiences and perceptions among stakeholders. A total of 76 responses were received online, plus one via email, covering all Member States except Greece and Poland; 68 responses came from law enforcement, 5 from judicial authorities, and 4 from the public administration officials.[36]

As explicitly noted by the European Commission, the survey focused on the collection of respondents' estimates, as it was clear that relevant data as such are *"not collected in Member States"*.[37] Thus, the survey did not seek to collect any quantitative input other than approximations or extrapolations shared by the respondents, presumably on the basis of their experience.

4.2.1 Qualitative input contextualising quantitative answers

Some estimations were indeed provided in the answers. A number of respondents, however, and in spite of making the effort of indeed completing the questionnaire, also manifestly and actively resisted the invitation to provide the estimations requested from them. This becomes is not particularly echoed in the Impact Assessment, but becomes more visible when analysing directly such answers.[38]

A number of questions in the document prepared by the European Commission, indeed, were directly formulated as requests for estimates ("*Please estimate the percentage of…"*,[39] "*Please estimate the breakdown per type of data…"),*[40] and gave the possibility to respondents to either select between a series of ranges of percentages, or to pick up the option "*I cannot estimate*", or "*I cannot indicate"*. When the latter answer was selected, respondents were encouraged to justify their choice in a subsequent question, with formulas such as "*Please explain why you cannot estimate the percentage(s) of the previous question*".[41]

---

[35] This survey is designated as 'target survey 2' in the Impact Assessment.
[36] Impact assessment, p. 135.
[37] Ibid., p. 130.
[38] The questionnaire ('*Survey to public authorities on cross-border access to e-evidence'*, Ref. Ares(2019)4117217 - 28/06/2019) and the answers submitted online were made accessible by the European Commission following a request for public access to documents submitted in June 2019. The provided copy of the answers does not include personal details such as names or email addresses; it also does not contain information about the organisations of the respondents who did not consent to the publication of their organisation's information; all respondents were requested to declare that nothing within their responses was unlawful or would infringe the rights of any third party in a manner that would prevent publication. All respondents were informed via the questionnaire that "*whatever option chosen…* [y]*our answers, excepting personal data, may be subject to a request for public access to documents under Regulation (EC) N°1049/2001*".
[39] For instance, Questions 10, 12, 16.
[40] For instance, Question 14.
[41] For instance, Questions 11, 13, 15, 17.

Some of the explanations provided by those who asserted it was not possible for them to share estimates include references to a lack of sufficient data about the phenomenon, including specific mentions of absence of detailed statistics,[42] which confirms the initial premise of the European Commission. Some responses refer to a lack of personal, direct experience on the matters being surveyed, which indeed affects the usefulness of any attempts to estimate. Importantly, some respondents also question the very possibility of confidently providing any valid estimates, for instance in light of the fact that the issues about which they are questioned are highly case-dependent, and that realities might vary depending on the type of crime, the circumstances of the crime, and the type and volume of data requested, or more generally for considering that certain estimations "*cannot seriously be rendered*".[43]

Nevertheless, the claims that the Impact Assessment submits, on the specific grounds of this survey, include utterances such as the following: "*More than half of total investigations include a request to cross-border access to e-evidence*", "*Less than half of all the requests to service providers are fulfilled*", and "*Almost two thirds of crimes involving cross-border access to e-evidence cannot be effectively investigated or prosecuted*".[44] Results of this survey, framed in these terms, were used for the section of the Impact Assessment which defines and assesses the "*magnitude of the problem*" allegedly justifying the legislative initiative.[45]

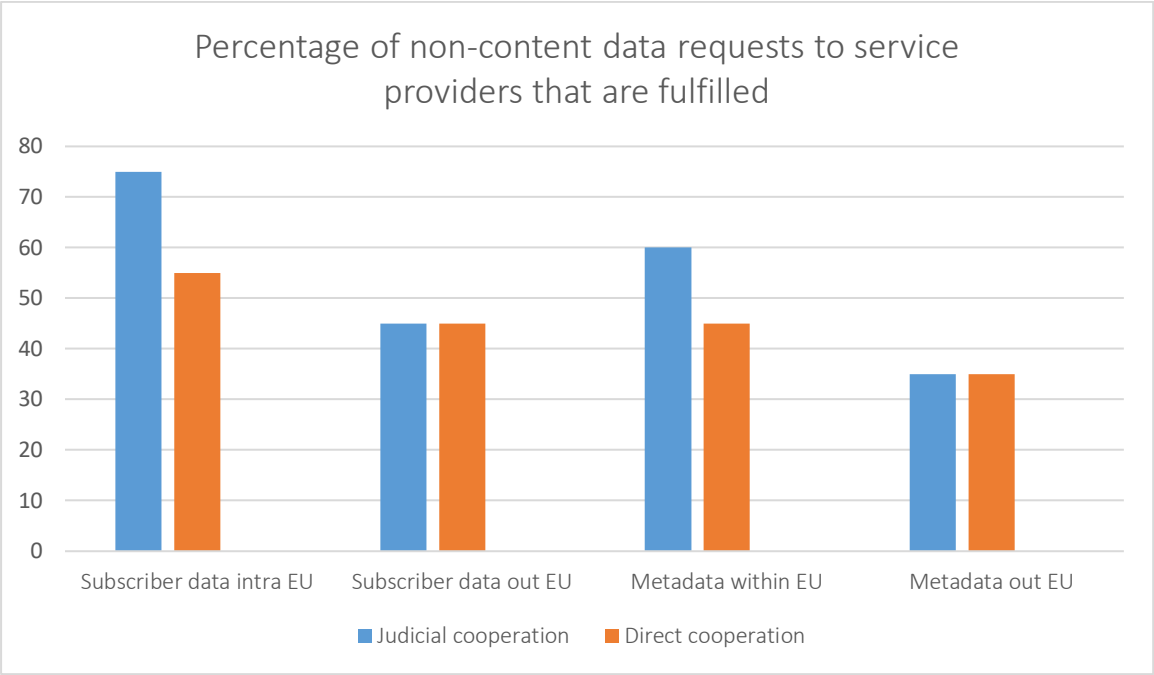
In light of the fact that the survey was aiming at merely collecting estimates, as well as qualitative information on such but also the different insights gathered from respondents on the actual difficulty of providing reliable estimates, it appears necessary to insist on the relativity of findings such as those highlighted in the Impact Assessment, or at least to the need to qualify them more openly.

4.2.2 Other readings

The survey did lead to results such as those illustrated in the below table, which compares the success-rate of requests for non-content data addressed to service providers depending on whether data are requested through judicial cooperation channels or by asking directly for the data to the service provider.[46]

[42] "*Cause we do not have records of such requests*", as expressed by one of the respondents.
[43] As stated in p. 62 of the document with answers provided by the EC.
[44] Impact Assessment, p. 130.
[45] Ibid.
[46] The figures used are those presented by the European Commission in Table 3, p. 16 of the Impact Assessment.

Table 1. Percentages of fulfilled requests (non-content data)



As shown in this table, according to the survey's results opting for requesting data directly to service providers does not increase the probability of the success of requests, on the contrary: requests for non-content data appear to be more effective when conducted through judicial cooperation channels in intra-EU scenarios, and just as effective as alternative solutions in scenarios involving extra-EU requests.

The Impact Assessment did not provide enough information to make similar comparisons in relation to requests for content data. Respondents were strongly reluctant to provide any answers to a question about "*the percentage of investigations where your request to a service provider located in a non-EU country is fulfilled*", in relation to content data from electronic communication services data and from other Internet or app-based services: almost 60%, on average, preferred not to give any estimated range of percentages about such investigations.[47]

Taking into account the focal importance of facilitating access to content data across the Atlantic in the policy push for the E-evidence package and related developments, the fact that a majority of consulted national experts across the EU were unable and/or unwilling to share with the European Commission even an approximation as to what could be the size of this specific problem is, certainly, to be highlighted.

[47] The average percentage of answers "*I cannot estimate*" and absence of answers to these sub-questions of Question 57, on the basis of the answers provided online, is 57,89 %.

5. Final remarks

Facilitating the access by public authorities to data held by private companies is, there is no doubt, high on the agenda of EU's institutions. The mantra according to which the fight against crime requires *faster* and *smoother* access to *more* data has manifested in a variety of ways, and is currently mainly embodied in three different initiatives – the E-evidence package, the negotiation of an EU-US Agreement, and the participation in negotiations on a Second Additional Protocol to the Cybercrime Convention.

These three initiatives are concerned with 'cross-border' access to data, in ways to as a matter of fact allow for a certain re-configuration of how jurisdictional borders and data flows interact and mutually shape each other.

Looking at the evidence beyond these developments, it surfaces that available information substantiating their necessity is fundamentally limited. Although this does not preclude as such that they might not be beneficial and useful to some extent, it renders particularly challenging the assessment of the strict necessity of any upcoming measures. More importantly, it renders extremely delicate any balancing between such – yet unquantified – need and the legal imperative to protect the fundamental rights and freedoms of individuals protected under EU law.

References

Carrera, Sergio, Gloria González Fuster, Elspeth Guild, and Valsamis Mitsilegas (2015), *Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights*, CEPS Paperback, CEPS: Brussels.

Clarke, Richard Alan, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein and Peter P. Swire (2013), "Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies", United States President's Review Group on Intelligence and Communications Technologies, December.

Council of the EU 2017), Final report of the seventh round of mutual evaluations on "The practical implementation and operation of the European policies on prevention and combating cybercrime", ST 12711 2017 INIT, Brussels, 2.10.2017,

--- (2019), General approach to 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, 6946/19, Brussels, 28.2.2019.

--- (2019), Addendum to the Recommendation for a Council Decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters - adoption, Brussels, 27.5.2019.

--- (2019), General approach to Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters, 10206/19, 11.6.2019.

Daskal, Jennifer (2016), "A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right", *Just Security*, February (https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/).

European Commission (2015), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions: The European Agenda on Security, COM(2015) 185 final, Strasbourg, 28.4.2015.

--- (2018), 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 final, Strasbourg, 17.4.2018.

--- (2018), 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 final, Strasbourg, 17.4.2018.

--- (2019), Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, Brussels, 5.2.2019.

--- (2019), Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), COM(2019) 71 final, Brussels, 5.2.2019.

European Data Protection Supervisor (EDPS) (2019), "Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence", Opinion 2/2019, 2.4.2019.

Kris, David (2015), "Preliminary Thoughts on Cross-Border Data Requests", *Lawfare*, September 28 (https://www.lawfareblog.com/preliminary-thoughts-cross-border-data-requests).

ABOUT CEPS

Founded in Brussels in 1983, CEPS is widely recognised as the most experienced and authoritative think tank operating in the European Union today. CEPS acts as a leading forum for debate on EU affairs, distinguished by its strong in-house research capacity and complemented by an extensive network of partner institutes throughout the world.

Goals

- Carry out state-of-the-art policy research leading to innovative solutions to the challenges facing Europe today
- Maintain the highest standards of academic excellence and unqualified independence
- Act as a forum for discussion among all stakeholders in the European policy process
- Provide a regular flow of authoritative publications offering policy analysis and recommendations

Assets

- Multidisciplinary, multinational & multicultural research team of knowledgeable analysts
- Participation in several research networks, comprising other highly reputable research institutes from throughout Europe, to complement and consolidate CEPS' research expertise and to extend its outreach
- An extensive membership base of some 132 Corporate Members and 118 Institutional Members, which provide expertise and practical experience and act as a sounding board for the feasibility of CEPS policy proposals

Programme Structure

In-house Research Programmes

Economic and Finance
Regulation
Rights
Europe in the World
Energy, Resources and Climate Change
Institutions

Independent Research Institutes managed by CEPS

European Capital Markets Institute (ECMI)
European Credit Research Institute (ECRI)
Energy Climate House (ECH)

Research Networks organised by CEPS

European Network of Economic Policy Research Institutes (ENEPRI)
European Policy Institutes Network (EPIN)