Vazquez Maymir, Sergi

Article

Anchoring the need to revise cross-border access to e-evidence

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Vazquez Maymir, Sergi (2020) : Anchoring the need to revise cross-border access to e-evidence, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 3, pp. 1-24, https://doi.org/10.14763/2020.3.1495

This Version is available at:
https://hdl.handle.net/10419/224939

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 3

Anchoring the need to revise cross-border access to e-evidence

Sergi Vazquez Maymir
Fundamental rights centre, Vrije Universiteit Brussel, Belgium, Sergi.Vazquez.Maymir@vub.ac.be

Published on 16 Sep 2020 | DOI: 10.14763/2020.3.1495

Abstract: In April 2018 the European Commission presented an e-evidence package including a Proposal for a Regulation on a European Production and Preservation Orders for electronic evidence in criminal matters and a Proposal for a Directive on the appointment of legal representatives. The e-evidence package was accompanied by an impact assessment. This assessment asserts that e-evidence is requested in half of all investigations (first premise), that the mutual legal assistance treaties (MLAT) system is an inefficient channel for that purpose (second premise), and that as a result, two thirds of crimes cannot be effectively investigated (third premise). I challenge the empirical soundness of these three findings and argue that the percentages and figures used frame the problem fundamentally on technical and efficiency grounds. There is no reference to the political and economic motivations behind the promotion of a policy shift from MLAT to direct cooperation, which in my view, is the fourth and lost premise.

Keywords: E-evidence, Impact assessment, Cross-border access requests, Judicial cooperation, Service providers

Article information

Received: 26 Sep 2019 **Reviewed:** 21 Dec 2019 **Published:** 16 Sep 2020

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/anchoring-need-revise-cross-border-access-e-evidence

Citation: Vazquez Maymir, S. (2020). Anchoring the need to revise cross-border access to e-evidence. *Internet Policy Review*, *9*(3). DOI: 10.14763/2020.3.1495

This paper is part of Geopolitics, jurisdiction and surveillance, a special issue of Internet Policy Review *guest-edited by Monique Mann and Angela Daly.*

INTRODUCTION: THE PREMISES DEFINING THE E-EVIDENCE PROBLEM

Today, all human activity generates data and therefore potential electronic evidence ("e-

evidence") for law enforcement authorities investigating or prosecuting crime. Since EU citizens' data is mainly processed by service providers and digital platforms headquartered in the US, its storage and location often depend on business architecture choices rather than a traditional investigative jurisdiction (see de Hert et al., 2018; Svantesson, 2017).

According to the European Commission (the Commission), in the EU "crimes cannot be effectively investigated and prosecuted because of the challenges in cross-border access to electronic evidence" (European Commission, 2018, p.9). These challenges are often linked to the channels currently used to request e-evidence across borders, which are regarded as cumbersome, too lengthy or simply inadequate. With the aim of improving cross-border access to e-evidence, in April 2018 the Commission presented the so-called e-evidence package, that included: a Regulation on European Production and Preservation Orders (EPOs) for electronic evidence in criminal matters (EPO Regulation); and a Directive on the appointment of legal representatives (LR Directive). In short, departing from a mutual legal assistance treaty (MLAT) model, the proposed e-evidence package presents new rules aimed at enhancing direct cooperation between law enforcement authorities (LEAs) [1] and service providers. [2]

On the one hand, the EPO Regulation grants EU authorities the possibility to issue production and preservation orders for e-evidence directly to service providers established in another EU member state. On the other hand, the LR Directive imposes the obligation on service providers [3] offering services in the EU to appoint a legal representative in order to receive, comply and enforce evidence requests from EU LEAs. [4] The package is accompanied by a regulatory impact assessment, an extensive report of 282 pages, drafted by the Commission.

Impact assessments are one of the most relevant tools available to EU institutions to reach well-informed decisions in policy making (Keyaerts, 2012; Alemmano, 2011). In the context of the Commission's legislative action, impact assessments belong to the set of common principles and processes, enumerated in its Better regulation: guidelines and toolbox. As such, impact assessments represent an instrument to support the justification of the EU's policy and legislative initiatives against claims of arbitrariness (Keyaerts, 2012). Among the objectives of a regulatory impact assessment, there is verifying that a problem exists, identifying who is affected by it, estimating the problem's scale, analysing its causes and consequences, and assessing the problem's evolution in the absence of EU policy intervention (Better Regulation Toolbox, 2017). Due to their authoritative and conferred probative value, regulatory impact assessments have the operational capacity to institutionalise views of reality and therefore help to justify or undermine particular policies. It is in that sense that impact assessments have been recognised as relevant tools by the Court of Justice of the European Union (CJEU) when examining the justification for EU legislation under necessity and proportionality criteria (Keyaerts, 2010; Alemanno, 2009).

In the case of the e-evidence package, the Commission's impact assessment defines the problem faced by LEAs when requesting access to e-evidence stored or located abroad based on the following three findings (European Commission, 2018):

1. More than half of all investigations include a cross-border access request to e-evidence;
2. Less than half of all the requests to service providers are fulfilled;
3. Almost two thirds of crimes involving cross-border access to e-evidence cannot be effectively investigated or prosecuted.

Each of these findings implies a premise that characterises the definition and the magnitude of the problem of investigating crime where e-evidence is involved. In that respect, the first finding

suggests a generalised need among law enforcement to access e-evidence across borders (first, or necessity, premise). The second finding suggests that MLATs are ineffective for cross-border access to e-evidence in criminal proceedings **(**second, or efficiency, premise). Finally, the third finding suggests a direct correlation between access to e-evidence and LEAs' capacity to fight crime (third, or impact, premise).

This paper does not focus on the content of the Commission's e-evidence package or its amendments, an exercise that has already been extensively carried by EU bodies (see Civil Liberties Committee, 2019; EDPB, 2018 or EDPS, 2019), academia (see Böse, 2018; Tosza, 2018; Christakis, 2020) and civil society organisations (see Fair Trials, 2018 or EDRI, 2019). Instead, the current contribution looks closely into each of the findings used by the Commission to define the problem of cross-border access to e-evidence. The objective is to challenge the proposal's contextual framework and ultimately provide alternative perspectives for its assessment. This contribution argues that the findings and premises used to define the problem of cross-border access to e-evidence inadequately shape its assessment, oversimplifying it and drawing conclusions based on implicit and unfounded assumptions. Based on these premises, the Commission's impact assessment favours a US-style policy shift towards direct cooperation with service providers to the detriment of existing mutual legal assistance arrangements between judicial authorities.

The discussion will be structured as follows: the first section will introduce the notion of e-evidence. The second section will briefly summarise the main aspects of the two channels currently used by LEAs to request cross border access to e-evidence: mutual legal assistance (MLA) and direct cooperation with service providers. Section three will look at the sources of the impact assessment. Having established these conceptual elements, section four will address and examine each of the impact assessment's findings and their implied premises.

THE CONCEPT(S) OF E-EVIDENCE

What does e-evidence mean? There is not currently a single harmonised definition of e-evidence. E-evidence is data in electronic form or computer data, that is, any representation of facts, concepts or information, stored or transmitted in binary form suitable for processing in a computer system or network. Anything can be "electronic data" and thus potentially e-evidence if digitised, or, in other words, turned into the binary form capable of being accessed, viewed and or processed by automatic means. In that sense, e-evidence might refer to: a) a physical object (e.g., the picture of a murder weapon); b) analogue generated information (e.g., a confession in a tape or video recorder); or ultimately, to c) computer generated data (e.g., the content of an email or its metadata) (Biasiotti, 2017).

The EPO Regulation, in Article 2(6), defines e-evidence as "evidence stored in electronic form by or on behalf of a service provider at the time of the receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data and content data". Alternatively, the glossary of the impact assessment defines e-evidence as "electronically stored data such as subscriber information, metadata or content data, generated by any activity related to digital services" (European Commission, 2018, p. 3).

Both definitions relate to stored data only and therefore exclude the interception of in-transit data. However, besides their similarities they also hold relevant differences that deserve further attention.

First, in the impact assessment e-evidence is defined as "electronic data", a neutral term that is alternatively replaced in the EPO Regulation by the notion of "evidence". In that way the Regulation grants a *prima facie* qualification of "evidence" to the data requested through it, and therefore acknowledges by default the probative value of electronic data in the context of criminal proceedings (European Parliament, 2019b, p. 147).

Second, in the EPO Regulation the material scope of e-evidence is delimited by reference to a narrowed list of service providers, while the impact assessment refers to a more general notion of "digital services". The EPO Regulation solely covers electronic data "stored or processed by or on behalf" of a service provider offering either electronic communication services, information society services or internet infrastructure services (European Commission, 2017, Article 2). The definition of these service providers is at the same time based on those definitions offered by the Proposal for a Directive establishing the European Electronic Communication Code and Directive 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services. Moreover, in the case of information society services, the EPO proposal excludes those for which the storage of data is not a defining component.

Third, the types of data identified in the two definitions of e-evidence differ. The impact assessment resembles the traditional categorisation of electronic communication data, separating content data and metadata (or non-content data), where metadata is further divided into traffic data and subscriber data (Warken, 2019). Instead, the EPO Regulation uses the notion of non-content data as an umbrella term to introduce two new subcategories, namely access data and transactional data. The impact assessment welcomes these new categories arguing that "leaving any of them outside the scope would greatly diminish the effectiveness of the initiative" (European Commission, 2018, p. 42). However, it must be recalled that there is as yet no legal precedent whereby access or transactional data have been singled out from metadata and turned into autonomous categories. This represents a discretionary choice of the legislator aimed at introducing tailored norms for LEAs' access to certain types of data.

The proposal's approach relies on two main assumptions. First, that access and subscriber data share an equivalent purpose and an equal level of intrusiveness (European Commission, 2017, Recital 21). Second, that some metadata is less sensitive than communication content, this being a contested claim that might conflict with the reasoning given by the Court of Justice in the *Digital Rights Ireland* and *Tele2* cases (see Kift & Nissenbaum, 2016; Warken et al., 2019, for discussion).

The definition of what e-evidence is has a central role in the justification of the European Commission's e-evidence proposal. The broadening or narrowing of the concept also limits or expands the perception of what the problem faced by authorities is, and consequently the necessity for a legislative initiative.

MUTUAL LEGAL ASSISTANCE MODEL VS DIRECT COOPERATION MODEL IN THE CONTEXT OF E-EVIDENCE

Today, LEAs seeking to access data located extraterritorially can either issue a request to the authorities of the foreign country where the data is located (via mutual legal assistance) or, if

their domestic laws allow it, directly approach the service provider in control of that data (via direct cooperation). Additionally, LEAs might bypass any intermediaries and obtain the data directly by gaining access to it. Due to its unilateralism, this last method will not be discussed here (see Koops & Goodwin, 2014, for discussion).

In the European Union, MLA rules can be found either in international agreements (such as the Council of Europe Convention on Cybercrime), bilateral agreements signed between member states or the EU with third countries such as the US. The MLA model is considered a "request model", as it allows the authority of a state (requesting state) to request from their counterparts in another state (executing state) the execution of a particular police or judicial measure. The procedure is subject to the provisions of the legal instrument invoked, which can determine which of the domestic laws of the requesting state (*forum regit actum*) or those of the executing state (*locus regit actum*) prevail (Klip, 2016).

Requests of electronic data between the EU and US authorities today remain subject to the provisions of the Agreement on Mutual Legal Assistance signed in 2003 (EU-US MLA Agreement, 2003), and the EU-US agreement on personal data protection (Umbrella Agreement) and any agreements that each member state has concluded bilaterally with the US (European Commission, 2018, p. 213).

Across the EU, cooperation in criminal matters between member states has progressively evolved into a qualified type of assistance named mutual recognition (Klip, 2016). Under mutual recognition, requests from the issuance state are given a "quasi-automatic" legal effect in the jurisdiction of the receiving or executing state (Larsen, 2018). To this day, the most recent example of mutual recognition instruments is the European Investigation Order Directive, which allows LEAs from one member state to request the execution of investigatory measures from the authorities of a second member state, including among others, the production and preservation of e-evidence. [5]

In the context of e-evidence gathering, and despite that its legal basis is highly controversial, some LEAs are increasingly approaching service providers outside the MLAT model. As its name indicates, under the direct cooperation model LEAs directly contact service providers without any intervention of the authorities of the country to which the request is sent. However, as observed in the 2016 Commission's Q uestionnaire on improving criminal justice in cyberspace, the effective fulfilment of a direct request remains uncertain: on one hand due to its unclear legal framework; and on the other hand, because of the difficulties in ensuring extraterritorial enforcement of domestic production orders.

There is currently no common position in the EU about the lawfulness of direct cooperation, a circumstance that came about for two main reasons. First, the differences among member states' regulation of domestic and foreign service providers. Second, due to the absence of rules on whether requests issued directly to a service provider in another country are voluntary or mandatory for the service provider being addressed. [6] In this context several connecting factors have been raised by LEAs to "hook" service providers into their jurisdiction. These arguments can generally be based on variations or expansions of claims aboutthe place where the service providers have their main seat, the place where the services are offered and the place where the data is stored (de Hert et al., 2018).

As will be further developed, there is a strong political trend promoting a paradigm shift towards direct cooperation between private companies and public authorities (González Fuster & Vazquez Maymir, 2020). The passing of the US Clarifying Lawful Overseas Use of Data

(CLOUD) Act in March 2018 embodies this political shift. Answering and rendering moot the questions posed by the Microsoft Ireland case, the CLOUD Act clarified that under US law, US authorities have the right to require the production of data processed by a service provider subject to US jurisdiction, regardless of where the data is stored or located (Stefan & Gonzalez-Fuster, 2018). On the signing of an executive agreement between governments, the CLOUD Act also contemplates the possibility that a US service provider directly answers requests of foreign countries for the interception or disclosure of data, including content data, under its control. All of this indicates that in the context of e-evidence, the new US framework will be used to circumvent the MLAT procedure by benefitting from direct cooperation with service providers. The signature of the US-UK Agreement and the current US negotiation of executive agreements with the EU and Australia, reinforce this political trend.

THE SOURCES OF THE IMPACT ASSESSMENT

To define the problem of cross-border access to e-evidence, the impact assessment attempts to quantify the volume of e-evidence requests and the number of investigations negatively affected by the alleged inefficiencies of MLAT and direct cooperation channels. The Commission recognises, however, that the endeavour has been heavily conditioned by the lack of data:

> It 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. Data at this level of detail is not collected by public authorities. There is no precise data available on the number of requests for judicial cooperation, direct cooperation, direct access or WHOIS lookups (European Commission, 2018, p. 13).

In the absence of reliable statistics the Commission grounds its analysis on estimations. With regard to mutual legal assistance in the EU, the impact assessment uses figures from the European Arrest Warrant and the European Judicial Network, estimating the existence of 13,000 yearly EU requests through MLAT/EIO of e-evidence between member states. For MLAT requests from EU to US authorities, the impact assessment uses the 2016 EU-US MLA review report, estimating 1,300 requests of e-evidence per year from EU authorities to their US counterparts (European Commission, 2018, p. 14).

Regarding direct cooperation, the Commission rests its analysis on the 2013-2016 transparency reports from five service providers, namely Facebook, Google, Microsoft, Twitter and Apple. According to these reports, the five companies received more than 90% of the 120,000direct cooperation requests sent to the US in 2016. What is more, of those, 70% targeted Google and Facebook only (European Commission, 2018, p. 258-266). Despite the fact that transparency reports are considered the main source of data on direct cooperation, the impact assessment acknowledges the impossibility of ascertaining whether their figures strictly refer to direct cooperation requests, or, on the contrary, if they also relate to domestic orders deriving from a previous MLAT request. In other words, the figures in the transparency reports ignore whether a request arriving at a service provider's headquarters is the result of an MLAT procedure, or if it originates from authorities in the same country requesting its execution (European Commission, 2018, p. 14).

Moreover, the Commission assumes that requests issued via MLAT only seek content data while those via direct cooperation solely target metadata (or non-content data). Although no further clarification is offered, the assumption seems to be based on the aforementioned incapacity for service providers to discriminate between judicial and direct cooperation requests, as well as on the unwillingness to recognise that content data is being requested via direct cooperation (European Commission Task Force, 2016).

To overcome these empirical limitations, the impact assessment supports its analysis with a survey addressed to the public authorities of EU member states (Gonzalez-Fuster & Vazquez-Maymir, 2020). In truth, the premises defining the problem of e-evidence as described in the impact assessment are fundamentally built on the results of targeted survey n°2 (TS2):a survey not publicly available, that was conducted online during 17 days in October 2017, and that received 76 responses from LEAs from all EU member states except Poland and Greece. [7] Since 52 out of the 76 respondents decided not to provide their country of origin, the representation of respondents based on member state origin cannot be provided.

With regards to the professional occupation of the respondents, 68 were police authorities, 5 were judicial authorities and 4 were public administration officials. The survey also shows a high representation of LEAs involved in the investigation or prosecuting of cybercrime (n=21), followed by authorities focused on financial crimes (n=16), and less prominently, in charge of terrorism (n=7), human smuggling (n=6), child sexual exploitation (n=5), and organised crime (n=4). [8]The over-representation of police officers and LEAs investigating crimes heavily dependent on data, together with the small size of its sample, alerts us to potential biases in the survey results.

The Commission describes the objective of TS2 as that of "collecting quantitative and qualitative information on the size of the problem concerning cross-border access to e-evidence through both judicial cooperation channels and direct cooperation between public authorities and service providers" (European Commission, 2018, p. 135). Consequently, despite the impact assessment presenting TS2 as a source of objectivity, the reality is that they only provide subjective estimations from a very narrow sample of participants. This circumstance limits the empirical evidence supporting the Commission's assessment, and should alone prevent us from deducing any categorical premises from it. Keeping this warning in mind, the analysis of the premises is nonetheless valuable for further understanding the problem of cross-border access to e-evidence.

THE FIRST, OR NECESSITY, PREMISE: THE MAJORITY OF CRIMINAL INVESTIGATIONS IN THE EU REQUIRE CROSS-BORDER ACCESS TO E-EVIDENCE

The Commission states that 85% of all criminal investigations require e-evidence and of that percentage, two thirds (65%) are said to involve a cross-border request to a service provider. As a corollary to both figures, the impact assessment establishes the first premise of the problem, that "55% of total investigations include a request to cross-border access to e-evidence" or in other words that "more than half of all investigations include a cross-border request to access e-evidence" (European Commission, 2018, p. 14). The quantification and measurement of the size of the problem is key when it comes to objectively determining LEAs' needs to access data. Therefore, we must ask, how does the Commission ascertain such numbers and how credible are

they?

Before digging into the percentages, it needs to be highlighted that the definition of e-evidence used in TS2 differs from that of the EPO Regulation or the impact assessment. TS2's glossary defines "electronic evidence" as "electronically stored data such as subscriber information, metadata (connection/traffic/location data) or content, generated by any activity related to electronic communication services, telecommunications and other internet or app-based services". Therefore, e-evidence is not confined to data stored by a number of service providers or to digital services but instead refers to a broader concept of "electronically stored data". Nevertheless, the Commission uses the figures from TS2 to infer the quantitative relevance of e-evidence as it is understood in the e-evidence proposal.

Based on the Commission's explanations and, while not explicitly mentioned, the total percentage of investigations requiring cross-border access to e-evidence has its statistical basis as the combination of responses to question 10 (Q10)and question 12 (Q12) on the TS2 (European Commission, 2018, p. 258). The two questions followed the same formula and offered participants the possibility to estimate between a range of percentages from 0-11% to 91-100%. As an alternative the questions also allowed respondents to express the impossibility of making an estimation.

In Q10 [9] the Commission asked participants to "estimate the percentage of investigations where electronic evidence (in any form) is relevant, e.g. as a lead". The median of the estimations is the source that allows the Commission to claim that 85% of criminal investigations require e-evidence. Similarly, in Q12, [10] participants were asked to provide estimations about the total number of investigations where "a request to a service provider in another jurisdiction is needed to obtain the evidence". The results of Q12 are used to state that two thirds (65%) of all criminal investigations requiring e-evidence are cross-border.

From the combination of the results from Q10 and Q12, the core of the first premise is established, namely that 55% of all criminal investigations include a cross-border request to access e-evidence. [11] It is worth stressing again that despite the Commission seemingly discussing percentages of the total number of investigations, the premise is built upon a median of estimations from a relatively small sample with a very specific professional background.

To be precise, when contrasting the responses to Q10 and Q12 with the participants' area of crime specialisation, we observe that the results are heavily conditioned by the responses from LEAs investigating cybercrime and financial crimes, two areas of crime that are arguably more reliant on accessing "electronically stored data".

As the actual volume of cross-border access requests cannot be determined precisely, the Commission supports its conclusions by reference to the figures offered in the transparency reports of the five main service providers. Without elaborating any further, the Commission states that the reports "provide an idea of the number of requests that the above percentages refer to" (European Commission, 2018, p. 14). However, taking into account the flaws already explained, the analytical value of the transparency reports cannot be taken for granted.

Through the first, or necessity, premise, the Commission indirectly establishes an objective need for accessing e-evidence in the investigation and prosecution of crime. However, the logical relationship between more than half of all criminal investigations involving a request for e-evidence and its relevance or usefulness in the proceedings remains unknown. If we were to acknowledge the percentages given and the cause-effect relationship between the increase of

cross-border access requests and the existence of a generalised need for data in criminal investigations, then further considerations are needed.

Looking at the figures in annex 11 of the impact assessment (European Commission, 2018, p. 265), we observe that from the total of 120,032 direct cooperation requests received by Facebook, Google, Microsoft, Twitter and Apple in 2016, 91,137 were submitted by Germany, France and the UK. [12] In other words, these three countries alone represent "three quarters of the total number of requests to the main service providers submitted by law enforcement authorities in the EU" (European Commission, 2018, p. 267).

When comparing the total number of direct cooperation requests issued by each of these three countries against their population, we observe that the UK, Germany and France issue approximately four requests to service providers for every 1,000 citizens. [13]This ratio doubles the EU average. In fact, only Luxembourg and Portugal (approximately 3 for every 1,000) and Malta (which reaches a surprising number of 10 requests for every 1,000 citizens) are above the average. [14] Why do these countries issue double the number of requests than their fellow member states - is it that they take crime more seriously? While this seems doubtful, the disparity might find a better explanation in other reasons such as the differences in national procedural criminal laws (European Parliament 2018, p. 25), the societal confidence in an efficient prosecution of crime by the authorities, the political relevance given to different types of crime, the reliance on preventive versus reactive policies for criminal investigation (European Commission, 2011), or simply the resources available to authorities and their training (Europol, 2019).

Rather than showing a generalised need to access e-evidence, what the analysis of the first finding suggests is certain LEAs' growing dependence on obtaining certain data held by some service providers. It also suggests the existence of discrepancies between the needs of LEAs and member states, and the important influence of their idiosyncrasies in the estimated volume of requests issued (European Parliament, 2019a, p. 4).

For the reasons outlined above, it cannot be sustained that "more than half of all investigations include a request for cross-border access to e-evidence", there is no evidence supporting that statement. The impact assessment fails to provide sufficient evidence to support the implicit connection between the large amount of requests issued by LEAs and the necessity of e-evidence in the investigation and prosecution of crime. Therefore, the first or necessity premise which states that "the majority of crime investigations in the EU require a cross-border access to e-evidence" must also be rejected.

THE SECOND, OR EFFICIENCY, PREMISE: MLAT IS AN INEFFICIENT CHANNEL FOR CROSS-BORDER ACCESS TO E-EVIDENCE

The second, or efficiency, premise suggests that MLAT is an inefficient channel to access e-evidence: a conclusion obtained from stating that "less than half of all the requests to service providers are fulfilled" (European Commission, 2018, p. 15).

The source behind the ratio of fulfilment is the responses given by participants to Q21, [15] Q33, [16] Q45 [17] and Q57 [18] of TS2. Each question asked public authorities to provide estimations of the

percentage of requests fulfilled during investigations, based on the scenarios and the different types of data covered in the survey. [19] Table 1 of the impact assessment shows a summary of TS2 results based on three parameters: i. the type of data requested; ii. the channel followed to issue the request (judicial cooperation or direct cooperation); and iii. the location of both the requested authority or the service provider targeted by a request (EU country or non-EU country).

Table 1: percentage of requests to service providers that are fulfilled (survey data). Source: European Commission (2018, p. 16).

		Within the EU		With non-EU Countries	
		Judicial	**Direct**		
Non-content data	**Subscriber data**	75%	55%	45%	45%
	Metadata	60%	45%	35%	35%
Content data		55%	N/A [20]	30%	N/A [21]
		Note: the median of the above responses is 45%			

In light of table 1, the impact assessment concludes that requests to service providers within the EU are fulfilled in a higher ratio than those issued abroad, and that subscriber data is easier to obtain than content data (European Commission, 2018, p. 259). [22]Also, the percentages are used to generate the median of 45% for fulfilment rates, which help imply the inefficiency of existing channels to access e-evidence across borders.

To assess the robustness of the median given in table 1, it is important to look at the number of TS2 participants which chose not to answer the questions at all. Taking into account the aggregated responses for all types of data (i.e. non-content data and content data), it can be observed that 27% of the participants did not provide any estimate for requests for judicial cooperation among EU authorities and that 34% did the same for cooperation for non-EU member states. With respect to direct cooperation requests to service providers located in the EU, there are 34% of non-responses, a percentage that reaches 54% of the sample for direct cooperation requests issued to non-EU countries. This means, for example, that for the estimations of fulfilment rates of direct cooperation requests to the US, the Commission uses the response to a question for which 42 out of 76 respondents did not provide an answer. The sample is again too small to draw any representative conclusion.

Again, to fill the empirical gaps of TS2, the Commission leans on the service providers' transparency reports. Despite the impact assessment warning about the differences between a request being answered and fulfilled, the Commission still interprets the median of percentages as an insight supporting the fulfilment rates previously estimated in table 1. To better evaluate the Commission's claim, it is worth having a closer look at the report released by Google, one of the two primary recipients of cross-border access requests for data (European Commission, 2018, p. 15). [23] Google's figures from 2016, the last year examined by the impact assessment, reveal an average 41.08% of answers to all the requests submitted by member states. What if Germany, France and the UK, the main issuers of access requests, are excluded? The global percentage of answers drastically drops to 18.07%.

The Google effect finds its explanation in the extremely low answer rate for certain member

states. The case of Hungary stands out. In 2016, none of the 225 requests issued by the Hungarian authorities to Google were answered by the company. A similar observation can be drawn based on the answer rates to Slovakian requests (2.20%) and, to a lesser extent, those pertaining to Ireland (21%), Romania (23.19%), Italy (27.23%), Malta (29.77%), Portugal (32.18%), or Estonia (31.86%). When compared to the answer rates for France (54.05%), Germany (52.85%) and the UK (76%), it is clear that Google answers a higher ratio of the requests from these countries (European Commission, 2018, pp. 258-266).

Facebook, Google, Twitter, Apple and Microsoft process e-evidence access requests by classifying a request as one of three categories: emergency disclosure requests, legal requests and reservation requests (European Commission, 2018). It is up to the company and its internal policies to assess which requests pertain to which category. From our analysis, and considering the impossibility of discerning between MLA and direct requests, it can be concluded that the internal policy of service providers on e-evidence requests has a substantial - if not decisive - impact on the production or not of the requested electronic data, and in turn in the efficiency of existing channels for accessing e-evidence.

The impact assessment fails to provide sufficient evidence to support the claim that MLAT is an inefficient channel for cross-border access to e-evidence. This is an overstated and unfounded claim.

THE THIRD, OR IMPACT, PREMISE: ACCESS TO E-EVIDENCE CONDITIONS THE SUCCESS OR FAILURE OF FIGHTING CRIME

The third and last premise establishes a direct link between access to e-evidence and the success or failure of effectively fighting crime. The premise is built on the finding that "almost two thirds of crimes involving cross-border access to e-evidence cannot be effectively investigated or prosecuted" (European Commission, 2018, p.17). But where does that percentage come from? The Commission again uses the responses obtained in TS2 and particularly the answers to questions to Q25, [24] Q37, [25] Q49 [26]and Q61, [27] asking participants to "estimate the percentage of investigations which are negatively affected or cannot be pursued" due to the "lack of timely access" or the "lack of access" to e-evidence.As in previous questions, all options comprised percentage ranges for each of the four different scenarios contemplated in TS2, also offering participants the possibility to indicate their inability to provide an estimate.

The results are succinctly displayed in table 2. Without elaborating, and by literally titling it in those terms, the Commission assumes that table 2 "demonstrates the percentage of investigations involving cross-border requests to access e-evidence that are negatively affected or cannot be pursued and its main cause" (European Commission, 2018, p. 17).

Table 2: percentage of investigations involving requests to access e-evidence across borders that are negatively affected or cannot be pursued. Source: European Commission, 2018, p. 17.

Cause	Within the EU		With non-EU countries	
	Judicial	Direct	Judicial	Direct
Lack of timely access [28]	35%	25%	45%	15%

Cause	Within the EU		With non-EU countries	
	Judicial	Direct	Judicial	Direct
Lack of access (access denied)	25%	25%	25%	15%
Other	15%	5%	15%	10%
Total	75%	55%	85%	40%

In that way, table 2 implicitly associates the estimated number of investigations negatively affected or abandoned and the channel used to issue an e-evidence request (European Commission, 2018, p. 17). From its figures, the Commission states that 75% of all investigations involving a request for data through judicial cooperation channels within the EU are negatively "affected or abandoned", a percentage that reaches 85% in the case of non-EU countries. Using the same logic, the impact assessment indicates that the negative impact on requests for direct cooperation in the EU is reduced to 55%, and to an even lower 40% in the case of direct cooperation requests targeting service providers from non-EU countries. Based on these percentages, the impact assessment infers that direct cooperation is a more efficient channel than MLAT (European Commission, 2018). The impact assessment does not provide sufficient evidence for the claim that MLAT as a channel for cross-border access to e-evidence is more negatively affected by lack of timely access than direct cooperation.

This conclusion also challenges two subjacent ideas that consistently frame the scope of the Commission's analysis of the problem and its drivers: [29] on one hand, the understanding of what a negative impact on an investigation is; and on the other hand, the assumption that accessing data is equally relevant for the investigation of any sort of crime regardless of the type of offence.

What is a negative impact? The impact assessment gives little insight as to what is to be understood as a negative impact on a criminal investigation. While the Commission identifies its causes in a lack of timely access or lack of access (see table 2), it also lumps together their consequences, obviating any reference to their intensity or nature. In this way, the assessment fails to separate between the cases where not having data or accessing it late causes a minor or redeemable drawback, and those when it is fatal or conclusive to the proceedings. Indeed, the Commission's framing of the problem helps establish a generalised cause-effect relationship between access to data and a prejudice to any sort of investigation and prosecution. However, while not having immediate access might indeed result in consequences where data is at risk of being erased or moved, it might be an overstatement to consider that timely access to data has an equal impact in all cases. The same reasoning could be applied with regards to the impossibility of accessing data at all.

Is (all/any) data equally relevant to the investigation of all types of crime? Very often, cross border access to data is considered relevant to any crime leaving a digital trace (European Commission, 2018, p.13). [30] Since the impact assessment does not clarify the type of offences motivating requests for the production or preservation of data, it fails to provide a reasoned assessment based on necessity criteria. The Commission extrapolates the investigatory needs of specific serious crimes such as cybercrime, terrorism, child exploitation or organised crime, to the investigation of crime in general.

Based on table 2, the Commission states that "almost two thirds of crimes involving cross-border access to e-evidence cannot be effectively investigated or prosecuted" (European Commission, 2018, p. 17). The empirical basis for this finding is insufficient. Even though on

some occasions data might be the only lead for the investigation of crimes, it is not clear that the sole existence of a digital trace should justify a generalised dependence of investigations on access to data. The formulation of the TS2 creates bias towards the identification of access or timely access to e-evidence as the main factor negatively affecting criminal investigations. Further research on this matter could provide a far more comprehensive picture of the size of the problem, allowing the better identification of needs and cases where data is actually determinant while also serving as a deterrent mechanism against abuse caused by unnecessary requests.

THE LOST PREMISE: THE POLITICAL SHIFT FROM MLAT TO DIRECT COOPERATION

The three premises described not only define the problem of cross-border access to e-evidence, they also determine what is to be considered as the problem's potential causes. The impact assessment asserts that e-evidence is requested in half of all investigations (the first premise), that the MLAT system is an inefficient channel for that purpose (the second premise), and that, as a result, two thirds of crimes cannot be effectively investigated (the third premise). These premises confine the assessment almost exclusively to the relevance of data and the obsolescence of existing channels for requesting it. There is no reference to the political and economic motivations behind the promotion of a policy shift from MLAT to direct cooperation, which in my view, is the fourth, and lost, premise.

As with many other aspects of global policy, the position of the US must be considered (see also Cartwright, 2020), all the more if we take into account how the market dominance of US service providers has translated into a worldwide dependence on US procedures for data access requests. As has been explained, over 90% of all cross-border access requests for non-content data target five service providers headquartered in the US (Microsoft, Apple, Google, Facebook, Twitter) (European Commission, 2018, p. 14).

The US Criminal Division's Office of International Affairs (OIA) is today the central authority through which LEAs issue MLAT requests to obtain evidence located in the US. [31] But this has not always been the case: before the centralisation of the OIA, whenever foreign authorities requested US assistance, this would require the involvement of US attorneys from as many districts as there were locations of potential evidence. The difficulties in determining the district court responsible for fulfilling requests, and the unclear wording on the court's "jurisdiction over the offence" caused confusion in routine MLA cases and represented a "waste" of the already scarce US Department of Justice (DOJ) resources (Congressional Record, Vol 155, pt 12, 2009).

According to the DOJ, since 2000 the number of requests from foreign authorities handled by the OIA has increased dramatically, particularly for those cases requiring access to data from service providers. During the 2000-2008 period, the OIA managed to deal with the surplus of requests without any additional resources. In 2009, the department reached its saturation point and started to accumulate a backlog (Department of Justice, 2015).

In the same year the Obama administration passed the Foreign Evidence Request Efficiency Act (FERE Act) as a response. [32] The FERE Act was conceived as a paradigm shift on how MLA requests were to be handled: it promoted the centralised processing of foreign evidence requests and allowed them to be directly handled by the OIA rather than through US attorneys' offices.

To that end, a venue in the District of Columbia was created with jurisdiction to issue court orders compelling the production of evidence sought by foreign authorities. However, the envisioned paradigm shift has been thwarted by a lack of investment, and most MLAT requests for evidence still rely heavily on US attorneys based on the location of evidence (Department of Justice, 2015, p. 24).

In practice, the OIA's increasing workload faced has been shouldered by a sustained shortage of personnel caused by the department hiring freeze (Department of Justice, 2015, p. 23). Additionally, the OIA has also been suffering from serious technological limitations. In 2015, the DOJ declared that the management system used for all the OIA's case work still "had not seen a significant upgrade since its implementation in 1999" (Department of Justice, 2015, p. 23). This has resulted in serious transparency and operational deficiencies, which impeded authorities to adequately track the progress of requests at each iterative step (Department of Justice, 2015, p. 24).

Finally, on top of insufficient staff and resources, the lack of training and expertise of both US and foreign personnel when dealing with e-evidence requests has been repeatedly raised as a cause of delays and unfulfillment. In this respect, the DOJ has stressed the problems of foreign authorities meeting the US's probable cause standard, a requirement found in the Fourth Amendment and relevant for conducting searches or receiving warrants, particularly in the case of requests involving the content of communication (Department of Justice, 2015, p. 27).

The limitations of staff, information technology and training facilitated the backlog situation which in turn led to the OIA's adoption of stringent criteria in managing cases. The OIA's refusal of requests on *de minimis* grounds sparked criticism from, and the frustration of, foreign authorities (Department of Justice, 2015, p. 26). In light of this, since 2015 the DOJ has been publicly demanding resources to perform an overhaul of the country's mutual legal assistance scheme. In the advent of the Snowden revelations, the DOJ justified the need to carry out the MLAT reform, arguing that not doing so would threaten the competitiveness of US service providers and the US model of internet governance (Department of Justice, 2015, p. 22).

The MLAT Reform would focus on three main areas: i) executing the centralisation model for the reception and allocation of MLAT requests among US authorities; ii) adequately staffing the OIA and upgrading its technological capacities; iii) the training and outreach of both staff and foreign counterparts (Department of Justice, 2015) [33].

Not even a year after the first steps were adopted, in its report on the President's budget for the fiscal year 2017, the DOJ stated "[t]he OIA has shown in just a few months that it can make tremendous strides and progress toward faster and more efficient international evidence sharing". Accordingly, the DOJ endorsed the possibility that a sufficiently resourced MLAT channel could solve the backlog and thus become an efficient model for cross-border e-evidence requests (Department of Justice, 2016, p. 23).

But in March 2018 the interest in the MLAT model faded away with the passing of the CLOUD Act by the Trump Administration. The CLOUD Act embodies a new approach towards international cooperation for e-evidence requests, promoting LEAs' direct cooperation with US service providers to the detriment of judicial cooperation procedures. In sum, this supposes the "outsourcing" of traditional State competences and the externalisation of their associated costs to private entities.

As the DOJ reports show, despite the policy shift often being justified on technical grounds or

complex legal questions, there is a much simpler explanation. As the European Commission declared, countries like the US simply "(…) would not necessarily see a need to invest more in procedures that, from their perspective, are superfluous" (European Commission, 2018, p. 83).

It is precisely when we focus on the subjacent interests behind cross-border access to e-evidence that the "problem of e-evidence" encounters what appears to be one of its main obstacles: the lack of political incentives to invest in the MLAT channel. A lack of incentives that is not exclusive to the US but also resonates with the situation of EU member states and their cooperation under mutual recognition. In this regard, the Commission questions the cost of investing in judicial cooperation as a policy option. Concretely, regarding requests under EIO, the Commission argues that it "may not be appropriate or necessary for all cases, especially when there is no link [to the investigation] with the receiving jurisdiction besides the seat of the service provider" (European Commission, 2018, p. 157). [34]

Neither the US nor some EU member states want to invest in the MLAT channel, a procedure that involves obligations that are not required under their national laws and thus are often deemed unnecessary to protect their respective sovereign interests (European Commission, 2018). The publication in October 2019 of the long-awaited US-UK Agreement confirmed the paradigm shift towards a new order where direct cooperation between law enforcement and service providers is to become the new standard (Christakis, 2019).

The reluctance of some EU member states to invest in judicial cooperation might not reflect well on the health of the EU's Area of Freedom Security and Justice, but in this case, it might be merely circumstantial, as the decision to weaken the MLAT channel comes from the other side of the Atlantic. The US, currently the location of five of the most important service providers, has chosen to favour direct cooperation to the detriment of MLAT and it does not seem that the EU is willing (or perhaps capable) to confront this policy shift.

CONCLUSION

The Commission's e-evidence package envisages a scenario where the investigation and prosecution of crime is heavily data-driven and where service providers become key actors in the e-evidence gathering processes. Currently, two models coexist for accessing e-evidence across borders: mutual legal assistance and direct cooperation with service providers. In the EU, the different approaches taken by member states and their national laws question the lawfulness of using direct cooperation, yet following the US CLOUD Act and the unfolding of the Commission's e-evidence package, this might very soon change.

Ensuring an efficient channel for LEAs to access e-evidence abroad is necessary, and it may not always be realistic to demand or even achieve a detailed picture of the problem as a prerequisite for any legislative initiative. However, it is equally important that unfounded assumptions do not shape new law. In an attempt to depict MLAT as an obsolete and inefficient channel for data access requests, the Commission disregards what is perhaps the main cause of such obsolescence: the absence of a global political compromise to foster cross border cooperation between law enforcement authorities. Or in other words, there exists a hegemonic political stance of transferring states' responsibilities in criminal matters to private companies on efficiency and economic grounds.

How do we assess LEAs' needs when it comes to accessing e-evidence? Which investigations are

more affected by access or lack of access to e-evidence? How are misuses and abuses identified and dealt with? Are authorities sufficiently prepared and resourced to adequately carry out their tasks? The fact that there is no answer to these questions should put us on alert, not only for the purposes of assessing the e-evidence package but for ensuring adequate supervision and accountability of LEAs' practices in the investigation and prosecution of crime whenever e-evidence is involved.

REFERENCES

Alemanno, A. (2008). The Better Regulation initiative at the judicial gate: A Trojan horse within the walls of the Commission or the way forward? *European Law Journal*, *15*(3), 382–400. https://doi.org/10.1111/j.1468-0386.2009.00467.x

Alemanno, A. (2011). A Meeting of Minds on Impact Assessment: When Ex Ante Evaluation Meets Ex Post Judicial Control. *European Public Law*, *17*(3), 485–505. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1899276

Bellovin, S. M., Blaze, M., Landau, S., & Pell, S. K. (2016). It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law. *Harvard Journal of Law and Technology*, *30*(1), 1–101. https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf

Biasiotti, M. A. (2017). A proposed electronic evidence Exchange across the European Union. *Digital Evidence and Electronic Signature Law Review*, *14*, 1–12. https://doi.org/10.14296/deeslr.v14i0.2337

Böse, M. (2018). *An assessment of the Commission's proposals on electronic evidence*. [Study; Research paper]. European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf

Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1494

Christakis, T. (2019, October 17). 21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (And an Explanation of How it Works – with Charts [Blog post]. *European Law Blog*. https://europeanlawblog.eu/2019/10/17/21-thoughts-and-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/#_ftn1

Christakis, T. (2020, January 21). E-Evidence in the EU Parliament: Basic Features of Birgit Sippel's Draft Report [Blog post]. *European Law Blog*. https://europeanlawblog.eu/2020/01/21/e-evidence-in-the-eu-parliament-basic-features-of-birgit-sippels-draft-report/

Council of the European Union. (2016). *Review of the 2010 EU-US MLA Agreement – Examination of draft texts, 7403/16*. https://www.statewatch.org/news/2016/jun/eu-council-usa-mla-agreements-draft-texts-7403-16.pdf

Council of the European Union, General Secretariat of the Council. (2016). *EU-US relations—Review of the 2010 EU-US MLA Agreement*. Council of the European Union. https://www.statewatch.org/news/2016/jun/eu-council-eu-usa-mla-9291-16.pdf

Department Justice, Criminal Division. (2015). *FY 2016 President's Budget*. https://www.justice.gov/sites/default/files/jmd/pages/attachments/2015/02/02/10._criminal_division_crm.pdf

European Commission. (2016). *Proposal for a Directive of the European Parliament and the Council establishing the European Electronic Communications Code (Recast)COM/2016/0590 final—2016/0288 (COD)*. EUR-Lex. https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=CELEX%3A52016PC0590

European Commission. (2017a). *Better regulation: Guidelines and toolbox.* https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_en

European Commission. (2017b). *Targeted survey No. 2: Survey to public authorities on cross-border access to e-evidence. (Retrieved from an access request carried by the author).* Ref. Ares.

European Commission. (2018a). *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.* EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN

European Commission. (2018b). *Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.* EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN

European Commission. (2018c). *Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final—2018/0108 (COD).* EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN

European Commission, Directorate-General for Research and Innovation. (2011). *Crime and deviance in the EU. Key findings from EU funded social sciences and humanities research projects* (Studies and Reports). Publications Office of the European Union. https://doi.org/10.2777/63953

European Data Protection Supervisor. (2019). *Electronic evidence in criminal matters. Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters.* European Data Protection Supervisor. https://edps.europa.eu/data-protection/our-work/publications/opinions/electronic-evidence-criminal-matters_en

European Digital Rights initiative. (2019). *Recommendations on cross-border access to data. Position paper on the European Commission's proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters* [Position paper]. European Digital Rights initiative. https://edri.org/files/e-evidence/20190425-EDRi_PositionPaper_e-evidence_final.pdf

European Parliament, Committe on Civil Liberties, Justice and Home Affairs. (2019a). *4th Working document (A) on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD.* https://web.archive.org/web/20200606045256/https://www.birgitsippel.de/wp-content/uploads/sites/128/2019/06/4th_WD_Relations_with_third_country_law__Part_A.pdf

European Parliament, Committe on Civil Liberties, Justice and Home Affairs. (2019b). *Draft*

report on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (Draft Report 2018/0108(COD)). European Parliament. https://www.europarl.europa.eu/doceo/document/LIBE-PR-642987_EN.pdf

European Parliament, & Council of the European Union. (2015). *Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (Text with EEA relevance) OJ L 241*. EUR-Lex. http://data.europa.eu/eli/dir/2015/1535/oj

European Union, & United States of America. (2003). *Agreement on Mutual Legal Assistance between the European Union and the United States of America, OJ L181//41*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:22003A0719(02)

Europol. (2019, December 20). *SIRIUS: European Union Digital Evidence Situation Report Cross-border access to electronic evidence* [Press release]. Europol. https://www.europol.europa.eu/newsroom/news/sirius-european-union-digital-evidence-situation-report-2019

Eurostat. (2019, July). *EU population up to over 513 million on 1 January 2019* [Press release]. https://ec.europa.eu/eurostat/documents/2995521/9967985/3-10072019-BP-EN.pdf/e152399b-cb9e-4a42-a155-c5de6dfe25d1

Fair Trials. (2018). *Cross-border access to electronic data* [Policy Brief; Consultation Paper]. Fair Trials. https://www.fairtrials.org/publication/cross-border-access-electronic-data

Foreign Evidence Request Efficiency Act Of 2009, Pub. L. No. 111–79 (2009). https://www.congress.gov/111/plaws/publ79/PLAW-111publ79.pdf

González Fuster, G., & Vazquez Maymir, S. (2020). *Cross-border Access to E-Evidence: Framing the Evidence* (No. 2020–02; CEPS Papers in Liberty and Security in Europe). Centre for European Policy Studies. https://www.ceps.eu/ceps-publications/cross-border-access-to-e-evidence/

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, No. C-293/12 and C-594/12, (Grand Chamber, European Court of Justice 2014). http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1

Judgment of the Court In Joined Cases C□203/15 and C□698/15, Tele2 Sverige AB (C203/15) v Post-och telestyrelsen, and Secretary of State for the Home Department (C-698/15) v T. Watson, P. Brice and G. Lewis, (Grand Chamber, European Court of Justice 2016). http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=828733

Hert, P., Parlar, C., & Thumfart, J. (2018). Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland. *New Journal of European Criminal Law*, *9*(3), 326–352. https://doi.org/10.1177/2032284418801562

Keyaerts, D. (2010). Ex Ante Evaluation of EU Legislation Intertwined with Judicial Review? Comment on Vodafone Ltd v. Secretary of State for Business, Enterprise and Regulatory Reform (C-58/08). *European Law Review*, *35*(6), 869–884.

https://www.researchgate.net/publication/297772927_Ex_ante_evaluation_of_EU_legislation_intertwined_with_judicial_review_Comment_on_Vodafone_Ltd_v_Secretary_of_State_for_Business_Enterprise_and_Regulatory_Reform_C-5808

Keyaerts, D. (2012). The Impact of Better Regulation in the Case Law of the European Court of Justice. *European Journal of Risk Regulation*, *3*(2), 241–247. https://doi.org/10.1017/S1867299X00002117

Klip, A. (2016). *European Criminal Law. An Integrative Approach* (3rd ed.). Intersentia.

Koops, B. J., & Goodwin, M. (2014). *Cyberspace, the cloud, and cross-border criminal investigation. The Limits and Possibilities of International Law* (No. 05/2016; Tilburg Law School Legal Studies Research Paper Series). Tilburg University, Tilburg Institute for Law, Technology, and Society; Center for Transboundary Legal Development. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263#

Larsen, L. B. (2018). Afterword(s) on Mutual Recognition and the respect for fundamental rights Revisited-Following the Judgement in Aranyosi and Caldararu. In C. Briere & A. Weyemberg (Eds.), *The Needed Balances in EU Criminal Law, Past, Present and Future* (p. 433). Hart Publishing.

Network, E. J. (2020). *Status of implementation of 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters*. https://www.ejn-crimjust.europa.eu/ejn/EJN_Library_StatusOfImpByCat.aspx?CategoryId=120

Parliament, E., Civil Liberties, C., Justice, & Affairs, H. (2018). *Criminal procedural laws across the European Union –A comparative analysis of selected main differences and the impact they have over the development of EU legislation*. https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282018%29604977

Stalla-Bourdillon, S., Papadaki, E., & Chown, T. (2016). Metadata, traffic data, communications data, service use information… What is the difference? Does the difference matter? An interdisciplinary view from the UK. In S. Gutwirth, R. Leenes, & P. D. Hert (Eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (pp. 437–463). Springer. https://doi.org/https://doi.org/10.1007/978-94-017-7376-8_16

Stefan, M., & Fuster, G. G. (2018). *Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and latest developments in the EU and the US* (No. 2018–07; CEPS Papers in Liberty and Security in Europe). Centre for European Policy Studies. https://www.ceps.eu/ceps-publications/cross-border-access-electronic-data-through-judicial-cooperation-criminal-matters/

Svantesson, D. J. B. (2017). *Solving the internet jurisdiction puzzle*. Oxford University Press. https://doi.org/10.1093/oso/9780198795674.001.0001

The United States Department of Justice. (2016). *FY 2017 Budget and performance summary*. https://www.justice.gov/about/fy-2017-budget-and-performance-summary

Tosza, S. (2018). The European Commission's Proposal on Cross-Border Access to E-Evidence. *Eucrim*, 212–219. https://eucrim.eu/articles/european-commissions-proposal-cross-border-access-e-evidence/

Warken, C., Zwieten, L., & Svantesson, D. (2019). Re-thinking the categorisation of data in the context of law enforcement cross-border access to evidence. *International Review of Law, Computers & Technology*, *34*(1), 44–64. https://doi.org/10.1080/13600869.2019.1600871

Foreign Evidence Request Efficiency Act, S. 1289, United States Senate, 111 (2009). https://www.govtrack.us/congress/bills/111/s1289

Whitehouse, S. (2009). *President Obama Signs Whitehouse Bill to Ease Burdens Imposed on U.S. Attorneys by Foreign Investigations* [Press release]. Sheldon Whitehouse, United States Senator for Rhode Island. https://www.whitehouse.senate.gov/news/release/president-obama-signs-whitehouse-bill-to-ease-burdens-imposed-on-us-attorneys-by-foreign-investigations

[Declaration of novelty and no competing interests]

By submitting this manuscript, I declare that this manuscript and its essential content has not been published elsewhere or that it is considered for publication in another outlet.

No competing interests exist that have influenced or can be perceived to have influenced the text.

FOOTNOTES

1. i. Judges; ii. Courts; iii. Investigating judges; iv. Prosecutors; and v. Any other competent authority acting in its capacity as an investigating authority (Article 4 of the EPO Regulation).

2. According to the EPO Regulation (Article 2(3)) service provider means any natural person that provides one or more of the following categories of services : i. Providers of electronic communication services (ECS); ii Information Society Services (ISS); iii. Internet Infrastructures Services (IIS).

3. According to LR Directive (Article 2(2)), service provider means any natural person that provides one or more of the following categories of services : i. Providers of electronic communication services (ECS); ii Information Society Services (ISS); iii. Internet Infrastructures Services (IIS).

4. Note that despite being part of the e-evidence package, the LR Directive does not limit itself to the notion of e-evidence enshrined in the EPO Regulation proposal. Instead, its material scope embraces all sorts of evidence and not only that strictly defined as “electronic”.

5. All member states have implemented the EIOD except Denmark and Ireland which opted out of its adoption and thus still rely on the previous MLAT, namely the EU Convention on Mutual Legal Assistance 2000 (European Judicial Network, 2020).

6. According to the survey, the majority of member states (17) consider voluntary the fulfilment of direct requests issued by LEAs to a service provider located in another country, while at least seven member states consider such requests to be mandatory.

7. The analysis in this contribution is based on an access request by the author: Ref. Ares (2019) 4117217 28/06/2019. Some details and findings from the survey can be found in Annex 2 and Annex 11 of the impact assessment (European Commission, 2018, p. 135, p. 258)

8. The figures relate to the responses to TS2 Q8 which asked the “Area of crime you focus on”.

Due to the open character of the question on some occasions responses referred in different terms to the same areas of crime. The analysis in this contribution presents harmonised responses and as such might show inconsistencies regarding the raw data.

9. Targeted survey nº 2, Question 10: Please estimate the percentage of investigations where electronic evidence (in any form) is relevant, e.g. as a lead.

10. Targeted survey nº 2, Question 12: Please estimate the percentage of total investigations in which you would need to make a request to a service provider in another jurisdiction (cross-border access, service provider headquartered outside your country) to obtain the evidence.

11. This results from calculating the 65% out of the 85% of the estimated total number of investigations requiring e-evidence.

12. Total number of requests in 2016 by country: Germany: 35,271, UK: 28,598; France: 27,268

13. According to Eurostat, 2019 Population: Germany 83,019,200; France 67,028,000; UK 66,647,100; Total EU: 513,477,632. Source: Eurostat (2019). EU population was over 513 million on 1 January 2019.

14. Note that one request might imply the disclosure of information about more than one individual, therefore this figure should not be interpreted literally.

15. Targeted Survey nº2, Q21: Please estimate the percentage of investigations where your request to service providers via public authorities of another EU member state is fulfilled.

16. Targeted Survey nº2, Q33: Please estimate the percentage of investigations where your request to service providers via public authorities of a non-EU country is fulfilled.

17. Targeted Survey nº2, Q45: Please estimate the percentage of investigations where your request to service providers located in another EU member state is fulfilled.

18. Targeted Survey nº2, Q57: Please estimate the percentage of investigations where your request to a service provider located in a non-EU country is fulfilled.

19. The types of data covered in each scenario were: 1. Electronic communication services data: subscriber information; 2. Electronic communication services data: metadata; 3. Electronic communication services data: content data; 4. Telecommunications data: subscriber information; 5. Telecommunications data: metadata; 6. Data from other internet or app based services: subscriber information; 7. Data from other internet or app based services: metadata; 8. Data from other internet or app based services; 9. Content data.

20. "Direct cooperation with service providers for access to content data is usually available for emergency situations only, which represent a very small number of total requests. Although the survey did not provide for sufficient granularity to indicate whether a request was related to an emergency situation, many of the respondents to this question came from counterterrorism units or were otherwise involved in serious crime areas that typically may give rise to emergency requests. Follow-up calls with individual respondents supported this assessment." (European Commission, 2018, footnote nº22).

21. Ibid.

22. The complete breakdown of all given responses is provided in Annex 11 Table 2: the

percentage of investigations where the data request is fulfilled.

23. Facebook and Google comprise over 70% of the total number of requests to the five main service providers.

24. TS2, Q25: Please estimate the percentage of investigations (with requests to public authorities in other EU countries to access e-evidence) which are negatively affected or cannot be pursued.

25. TS, Q37: Please estimate the percentage of investigations (with requests to public authorities of non-EU countries to access e-evidence) which are negatively affected or cannot be pursued.

26. TS2, Q49: Please estimate the percentage of investigations (with requests to service providers located in another EU member state to access e-evidence) which are negatively affected or cannot be pursued.

27. TS2, Q61: Please estimate the percentage of investigations (with requests to service providers located in non-EU countries to access e-evidence) which are negatively affected or cannot be pursued.

28. I.e. data not provided in time causing e.g. the disappearance of other leads. (Footnote n°24 European Commission, 2018, p. 17)

29. In section 2.1.3 of the impact assessment titled "Why is it a Problem", the Commission states "(a)after the crime has been committed: electronic evidence is volatile and can be transmitted, altered or deleted easily. Public authorities therefore need effective and timely access to it to be able to prosecute criminals and prevent future crimes(...)." (European Commission, 2018, p. 9)

30. In that respect, the Commission states: "The problem affects all types of crime that can leave a digital trace: it is relevant for many types of serious crimes, but also for a number of lower-impact, high-volume crimes such as spreading of malicious software (e.g. ransomware), but also when the only digital element is some form of electronic communication. It is relevant for the gathering of evidence for specific and individual criminal investigations and for specific and limited data access, rather than for other purposes that might require bulk data access". (See European Commission, p. 13)

31. In addition to the coordination of data access requests from both US and foreign authorities, the OIA is also entrusted with the preparation of extradition requests, preparation of requests for all types of evidence and witnesses, negotiation of extradition treaties and MLATs with the Department and the formulation of criminal justice policy.

32. Foreign Evidence Request Efficiency Act, S. 289—111th (2009).

33. "The MLAT handling process must be overhauled in a comprehensive and responsible manner to address the globalisation of crime and growth of electronic communications, and to ensure U.S. law enforcement retains the ability to seek reciprocal assistance from foreign partners. Just as critical is our need to safeguard U.S. security and economic interests that have become threatened by foreign frustration with a U.S. predominance of the Internet that is coupled with a perceived U.S. unresponsiveness to foreign authorities' need for U.S.-based evidence" (Department of Justice, 2015, p. 28)

34. "Some [member states] have not invested sufficient resources to keep up with the growth in

foreign demand, given that there is no own interest in the relevant investigations and the service is provided out of courtesy to the foreign country. This has further contributed to the delays in responses" (European Commission, 2018, p. 157).