EUROPOL

SIRIUS - CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE

SIRIUS EU Digital Evidence Situation Report 2019

Cross-border access to electronic evidence

EDOC# 1073582

The Hague, 20 December 2019

WWW.EUROPOL.EUROPA.EU/SIRIUS

SIRIUS@EUROPOL.EUROPA.EU

The SIRIUS Project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under grant agreement No PI/2017/391-896.

This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

EUROPOL

SIRIUS

Contents

Acronyms

- BSI: Basic Subscriber Information
- EDR: Emergency Disclosure Requests
- EIO: European Investigation Order
- EU: European Union
- FPI: Foreign Policy Instruments
- IP: Internet Protocol
- JHA: Justice and Home Affairs
- LEA: Law Enforcement Authority
- MLA: Mutual Legal Assistance
- MLAT: Mutual Legal Assistance Treaty
- OSP(s): Online Service Provider(s)
- UK: United Kingdom
- US: United States
- VLB: Valid Legal Basis

List of Figures

1. About the SIRIUS project

The SIRIUS project is a response to the increasing need of European Union (EU) authorities to access electronic evidence from foreign-based Online Service Providers (OSPs), in the context of criminal investigations. Spearheaded by Europol's European Counter-Terrorism Centre and European Cybercrime Centre, in close partnership with Eurojust and the European Judicial Network, SIRIUS aims to help investigators and judicial authorities to cope with the complexity and the volume of information in a rapidly changing online environment. The project's focus is to foster knowledge-sharing through events and training, as well as through a restricted platform, where practitioners from all Member States (MS) and third countries with operational agreement with Europol can find up-to-date information regarding cross-border access to electronic evidence.

In 2018, the project received funding from the European Commission's Service for Foreign Policy Instruments (FPI) to support the implementation of the EU-US Mutual Legal Assistance Treaty (MLAT) and the practical measures on cross-border access to electronic evidence agreed by the Justice and Home Affairs (JHA) Council in June 2017.

2. Aim and Scope of this report

The aim of this report is to draw a picture of the status of access of EU Member States to electronic evidence held by foreign-based OSPs in 2018. More specifically, the following components fall within the scope of this document:

1 / The volume of requests from EU Member States to OSPs;
2 / The main reasons for refusal or delay of EU requests;
3 / The main challenges in the process, from the perspective of the different stakeholders.

Due to the challenges in accessing comprehensive data relating to electronic evidence, the ambition of this report is not to provide an exhaustive assessment of such a complex field, rather to cluster data on cross-border access to electronic evidence coming from different sources. To the authors' knowledge, this is the first time such an exercise is carried out in a systematic way and including survey with judicial authorities, law enforcement from all EU Member States and input from over 12 OSPs.

The working definition of "Online Service Provider" used in this report is *any company providing online services to EU citizens*. The report is covering mainly OSPs established in the United States (US) or their legal entities based in the EU; their transparency reports collect statistics on requests addressed to both jurisdictions.

A *requesting country* is considered to be the country submitting any type of request for electronic evidence; an *enforcing country* is considered the country processing the judicial request for mutual legal assistance.

Ultimately, the report identifies areas and actions that could contribute in the short and long term to smoother cross-border requests, as its findings could potentially be used to:

1 / Inform decision-making;
2 / Create training programmes targeting law enforcement and judicial authorities;
3 / Contribute to the standardisation of policies and transparency reports from OSPs.

3. Methodology

3.1 Data collection

The present report has been developed with information collected from different sources, as listed below.

1 / **Information from companies' publicly available transparency reports regarding governmental requests for data disclosure**

Such transparency reports usually cluster data temporally into semesters and geographically into countries.

The transparency reports analysed for the purpose of this report were of the following OSPs: **Airbnb, Apple, Automattic, Cloudflare, Dropbox, Facebook, Google, LinkedIn, Microsoft, Oath, Snapchat and Twitter**. The selection of the companies was based on the relevance of the data held with respect to criminal investigations and on the availability of the reports. Certain companies, such as Amazon, Booking.com, Ebay, Paypal, Telegram, Uber and Viber, do not publish transparency reports regarding data requests specifically from EU authorities or about EU citizens.

2 / **Online surveys with EU law enforcement and judicial authorities**

Europol conducted a survey amongst EU law enforcement agencies, through a password-protected online form. The consultation lasted for 45 days, from 01 August 2019 to 15 September 2019 and led to 177 anonymous responses from representatives from all 28 EU Member States. The full questionnaire is available in Annex 1.

The European Judicial Network and Eurojust adapted the survey to the target group of judicial authorities and disseminated it to the contact points of the European Judicial Network and European Judicial Cybercrime Network at a MS level, and to EU judicial authorities. The survey was conducted through a password-protected form; the consultation lasted for 45 days, from 01 August 2019 to 15 September 2019 and 77 responses were collected from EU Member States representatives (no responses were received from representatives of Estonia, Luxembourg, Malta and Romania). The full questionnaire is available in Annex 2.

3 / **Interviews with Online Service Providers**

Europol engaged via face-to-face meetings, phone interviews and/or e-mail exchange with representatives from Airbnb, Apple, Dropbox, Google, LinkedIn, Microsoft, Snapchat, Twitter and Verizon Media (formerly known as Oath) for the purpose of this report.

The main topics discussed with these companies were:

- The main reasons for refusal or delay in processing of requests from EU authorities;
- The challenges in the electronic evidence process from the perspective of OSPs.

The findings based on these interviews should not be taken as the official position of any of the mentioned private entities or of Europol.

3.2 Limits of the report

The legal and technical complexity of this field makes it very hard to provide an exhaustive picture. Several methodological problems were faced during the drafting of this report, namely:

1 / At Member State level - while increasingly common in criminal and civil cases, requests for electronic evidence to foreign-based OSPs are submitted by several law enforcement and judicial authorities in each MS. Centralised statistics about such requests from law enforcement and judiciary authorities are often not collected or available for analysis.

2 / At OSP level – only a limited number of companies publish transparency reports about the EU governmental requests they receive and comply with. In addition, they often use different methodologies, definitions and breakdown of data. For example, some of the companies might distinguish criminal cases from civil cases or separate requests for content and non-content data, while others will not. From a methodological perspective, most companies cannot affirm with certainty the number of MLA requests received, because in most instances the court order or search warrant issued by the local authority may not indicate that it is the result of an MLA request. Therefore, since the country where the request is originated is generally not identified, requests may be counted and reported under the figures of the enforcing country.

4. Context

4.1 Electronic evidence today in the European Union

The internet has deeply shifted the way evidence is stored

Changes in policy are underway in the EU

At present, there are different ways to request lawful cross-border access to data

The internet plays a central role in people's lives today and it has completely transformed the way data is stored and transferred. The use of messaging apps for text and calls, social media, cloud storage and file sharing platforms has changed how people interact with family, friends, companies and colleagues. Nowadays, while safeguarding the right to privacy within the EU, authorities need to rely on information held by private companies to effectively investigate and prosecute crimes.

Requests for information from OSPs might be the only way to obtain decisive evidence in relation to stolen devices, credit card fraud and identity theft, for example, but it can also be fundamental in nearly any type of investigation, including missing persons, kidnapping, human trafficking and terrorism. From a law enforcement perspective, the internet has deeply shifted the way evidence is stored. Investigations that would traditionally be conducted within the borders of one country have now acquired an international dimension. It is not unlikely that the victim, the perpetrator, and the infrastructure where electronic evidence is located, or where the service provider exploited is, are all in different countries.

Legislation in this regard varies from country to country and different international legal instruments may be applicable. The Budapest Convention on Cybercrime[1] provides one of the most recent international legal frameworks for cross-border access to electronic evidence and represents a big step in facing the new challenges imposed by the use of the internet for criminal purposes.

Changes in policy to improve and expedite the process to request cross-border access to electronic evidence are underway in the EU, as the European Commission[2], the Council of the European Union[3] and the European Parliament[4] are engaged in a legislative procedure in this regard. Negotiations with third countries such as the United States, as well as in relation to the 2nd additional protocol to the Budapest Convention[5] are also ongoing.

[1] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[2] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en
[3] https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/
[4] https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-cross-border-access-to-e-evidence
[5] https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

4.2 Types of request from EU Member States to foreign-based Online Service Providers

At present, there are different ways to request lawful cross-border access to data held by OSPs in the context of criminal investigations. EU authorities may use either direct requests for voluntary disclosure or judicial cooperation under international agreements, depending on the type of crime being investigated, as well as other legal requirements. Legislation in this regard varies from country to country. The processes for requests from government authorities to private companies also vary according to the type of data sought and how sensitive it is. **Data stored by OSPs is generally classified in *Basic Subscriber Information*** (BSI) (e.g. name, phone number, e-mail address), ***Traffic Data*** (e.g. IP addresses, connection logs, metadata) and ***Content Data*** (e.g. content of e-mails and messages, photos). The definition of the data types can be found in several legal instruments, like for example the Budapest Convention on Cybercrime. However, OSPs collect data in different ways, according to their business needs and types of services, which lead to different interpretations of data categories.

The types of cross-border requests that governmental authorities may submit to access electronic evidence are further explained below.

4.2.1 Direct requests

A direct request based on voluntary cooperation between authorities and a foreign-based OSP is **frequently the fastest channel to lawfully obtain non-content data (BSI and traffic data) in the context of criminal investigations**. Due to the voluntary nature of such cooperation, companies may choose not to comply with such requests. In addition, direct requests must be submitted by the requesting country in accordance with its domestic legislation, whereas the OSP, when responding, must take into account the domestic legislation of the country where the legal entity of its data controller is based. Therefore, companies may set their own requirements regarding requests from foreign authorities, taking into consideration applicable laws, but also the particularities of their services and products.

4.2.2 Emergency disclosure requests

Emergency disclosure requests (EDR) are a type of direct requests for voluntary cooperation through which **companies may provide non-content data to foreign law enforcement and judicial authorities in an expedited manner, even in a matter of minutes or hours**. For OSPs based in the US, legislation defines an emergency as a situation "involving danger of death or serious physical injury to any person"[6] which requires "disclosure without delay of information"[7]. Since this is a type of voluntary cooperation, OSPs have their own policies and requirements for emergency requests from foreign-based authorities and typically ask authorities to provide as much context as

[6] 18 U.S. Code § 2702 section c.
[7] Ibid.

possible about the investigation and justify why immediate access to specific set of data is required.

4.2.3 Judicial cooperation requests

Requests though judicial cooperation are submitted by the judicial authority of one country to their counterpart in the other country, pursuing provisions established under bilateral or multilateral treaties and regulations (e.g. Mutual Legal Assistance treaties, European Investigation Order directive, Budapest Convention on Cybercrime). This type of request involves the judicial authorities of both the requesting country and the judicial authorities of the enforcing country. **Requests through judicial cooperation are necessary when foreign authorities are seeking disclosure of content data, when non-content data could not be obtained via other means, or in case domestic legislation establishes that this is required for admissibility of data as evidence in judicial proceedings.**

5. Findings

Over 74% of requests to eight major OSPs in 2018 originated in three Member States

Success rate of EU requests to eight major OSPs in 2018 was 66%

5.1 Analysis of transparency reports

5.1.1 Volume of data requests per country and per Online Service Provider

The analysis of transparency reports of Airbnb, Apple, Facebook, Google, Microsoft, Oath, Snapchat and Twitter (referenced in section 7) showed that the MS which submitted the highest number of requests in 2018 were Germany (67,991 requests), France (33,520), the UK (31,525), Spain (11,446) and Italy (9,653), with Germany and France representing more than half of the requests from the EU. Member States making the lowest number of requests were Cyprus (28), Bulgaria (64) and Latvia (73). The majority of requests were sent to Facebook (30%), Google (26%) and Apple (24%).

Figure 1 - EU Law Enforcement Data Requests to Major Online Service Providers in 2018, per Member State

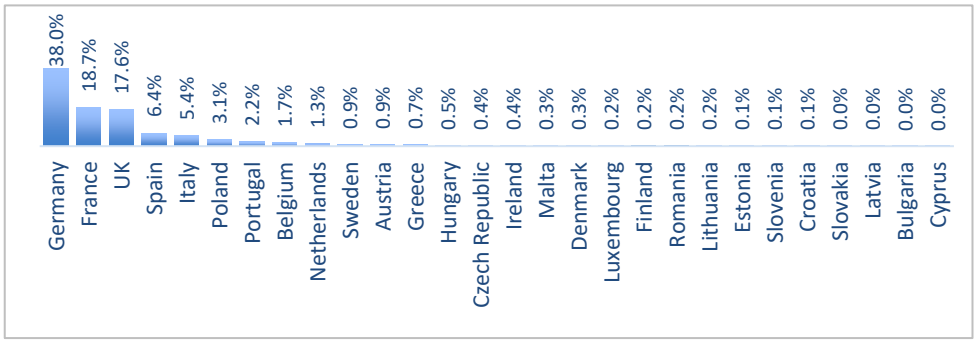
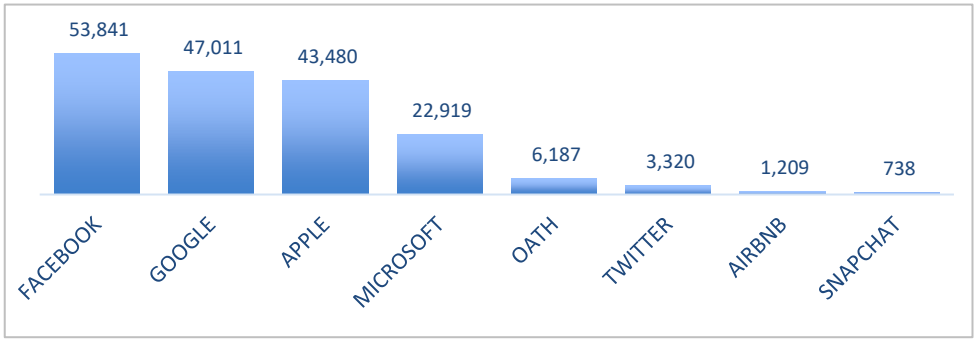


Figure 2 - EU Law Enforcement Data Requests to Major Online Service Providers in 2018, per company



The analysis of transparency reports from Automattic (which received 43 requests from EU authorities in 2018), Dropbox (22) and LinkedIn (39) demonstrated that the number of requests from EU authorities to these companies was relatively low in 2018, and very little or no data was provided[8].

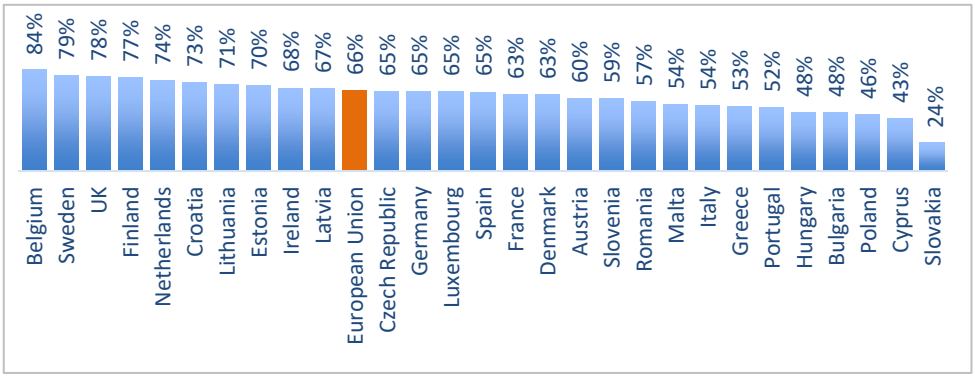
[8] According to publicly available transparency reports, Automattic did not produce any data in response to EU requests in 2018, Dropbox produced data in response to one request from the UK and LinkedIn produced

One of the reasons for the low number of requests to these companies is the fact that according to their policies, data may only be produced directly to foreign-based authorities in emergency cases. For all other types of investigations, formal judicial cooperation (e.g. MLA request) is required, even for non-content data, including BSI and traffic data.

5.1.2 Success rate

The success rate of data requests represents the percentage of requests for which some data was provided. In the EU, the overall success rate was calculated at 66%, taking into account data requests addressed to the eight OSPs mentioned above. This indicator has been calculated by dividing the amount of requests in which data was disclosed per total amount of requests received by the companies in 2018, as stated in their transparency reports[9]. Germany, the country that made 38% of all the requests in the EU in 2018, had a success rate of 65%, while France had a 63% success rate and the UK 78%. The reasons why requests from EU authorities for data disclosure were rejected by OSPs vary. The most frequent ones will be further explained in section 5.4 of this report.

Figure 3 - Success rate of EU Law Enforcement Data Requests to Major Online Service Providers in 2018, per country



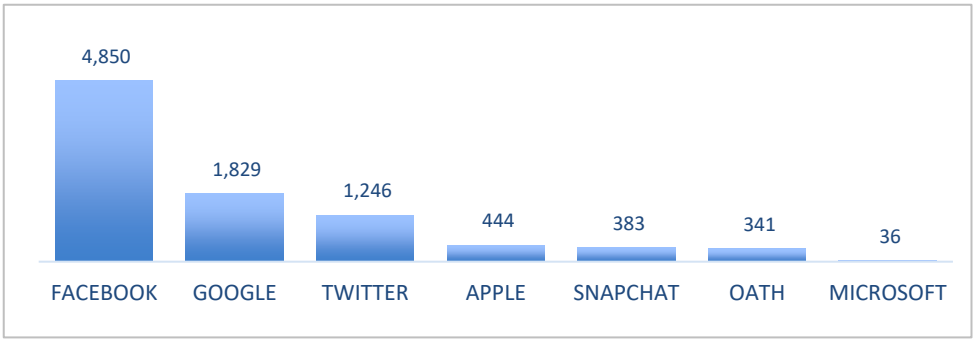
In investigations involving immediate threat to life or serious physical injury to any person, imminent and serious threat to the security of a State, the security of critical infrastructure or installation or crimes involving minors, it is possible for EU law enforcement to send EDR to OSPs based outside of the requesting country, depending on the jurisdiction. This type of request was used the most by the UK (6,158 emergency requests), followed by Germany (749) and France (705). Only Latvia did not submit any EDR to the companies analysed in this report in 2018. The company that received most of the emergency requests was Facebook (53%), followed by Google (20%) and Twitter (14%).

data in response to a number of requests. The authors of this report were unable to calculate the number of requests to which LinkedIn produced data, since the company reports on the percentage of accounts that were concerned by responses.

[9] The total number of requests and the number of requests where some data was disclosed regarding Apple was calculated by summing up the Device requests, Financial requests and Account requests data.

Figure 4 - EU Law Enforcement Emergency Data Requests to Major Online Service Providers in 2018, per Member State

Figure 5 - EU Law Enforcement Emergency Data Requests to Major Online Service Providers in 2018, per company



5.1.3. Compliance with requests

In its transparency report published in October 2018, Airbnb states that whenever it identifies a "legal deficiency" in a formal request for user information (including those related to non-disclosure requests), the company informs the requesting LEA about the deficiency, indicating the appropriate process to resolve the issue. All figures related to the rejection of requests for information refer to instances in which the relevant law enforcement officer decided not to pursue the request after being informed of the applicable legal deficiency.

Apple also emphasizes the internal review carried out by its legal team to ensure that each request has a valid legal basis; if the team determines that a request "does not have a valid legal basis … [or is] unclear, inappropriate and/or overly-broad (e.g. if it considers the scope of data requested as excessively broad for the case in question), we challenge or reject it". No indication is given, however, regarding the response provided by the LEA in charge of the request.

Cloudflare states that it will challenge "law enforcement requests [whether inside or outside the United States] that we believe are overbroad, illegal, or wrongly issued, or that unnecessarily restrict our ability to be transparent with our users".

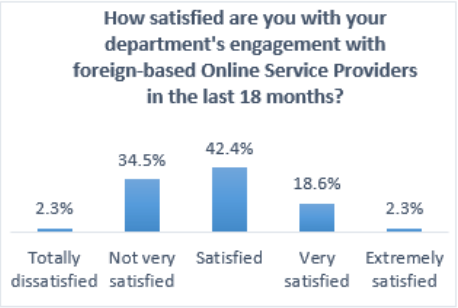
As an explanation to its category "No information provided", Dropbox states as possible reasons: a) the request was a duplicate; b) the company objected to the request; c) law enforcement withdrew the request; d) the request failed to specify an account. In addition, in the first semester of 2018, Dropbox received three requests for information addressed to the wrong company (it is not disclosed whether they were originating from the US or from other countries worldwide).

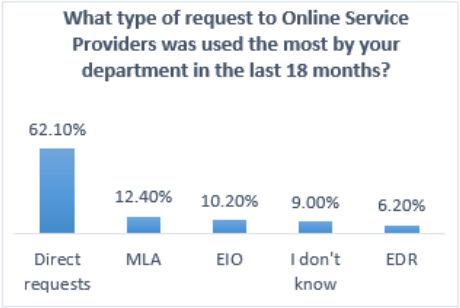
Twitter states that it rejects requests that are "improper", which it defines as including "invalid or overbroad legal process". More examples are provided: "a) we may not comply with requests that fail to identify a Twitter, Vine, and/or Periscope account or other content on those platforms; b) we may seek to narrow requests that are overly broad; c) users may have challenged the requests after we've notified them; d) we sought additional context from the requester and did not receive a response; e) in other cases, Twitter may challenge the request formally through litigation or informally through discussion directly with government entities".

5.2. Survey with EU law enforcement authorities

5.2.1. Engagement of EU law enforcement with foreign-based Online Service Providers

Over 60% of respondents say they are satisfied, very satisfied or extremely satisfied with their departments' engagement with foreign-based OSPs. 62% of respondents say the type of request used the most by their department for obtaining electronic evidence from OSPs is direct requests for voluntary cooperation. 12.4% say MLA and 10.2% say EIO are used the most. EDR was mentioned as the main type of request by 6.2% of respondents.





Respondents were also invited to evaluate the current process to lawfully request data disclosure from foreign-based OSP in open text. Some of the answers[10] were:

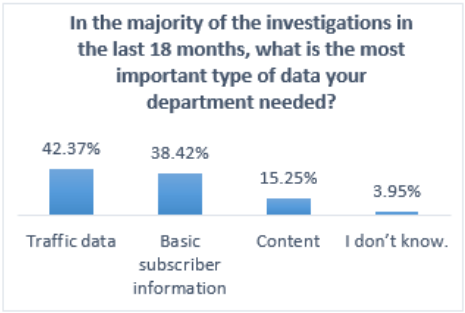
- *It's good but we need a global law/cooperation for all the companies to be cooperative and have the same rules. I think the process regarding online portals is good, and could be improved, but the biggest issue remains the time it takes to receive an answer (especially*

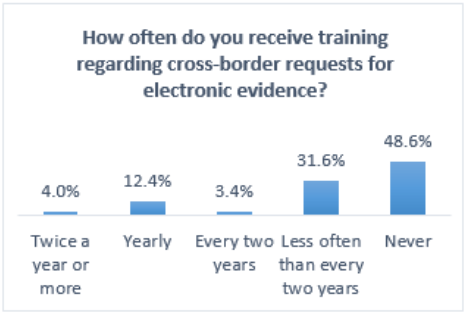
[10] Responses were edited for clarity.

with emergency requests). Long judicial steps to receive content from these companies are also a big restraint. It leads almost every time to not requesting the data at all, because of the time frame.

- *It's easy and quick, but many people are unaware of these procedures.*
- *Cumbersome, overly complex and excessively slow.*
- *Every OSP has its own procedure to reduce their own workload. This results in a huge variety of different requests for a SPOC[11] to manage. It would be great if there could be any possibility of automatizing those procedures for most of them.*

In the majority of investigations, the most needed type of data according to respondents is Traffic Data (e.g. connection logs, IP addresses, number of messages), followed by Basic Subscriber Information (e.g. name, e-mail, phone number), and only then content data (e.g. photos, mail/messages content, files). Regarding specific training about cross-border access to electronic evidence, 48.6% say they never received any training and 16.4% replied they receive specific training on the matter at least once per year.

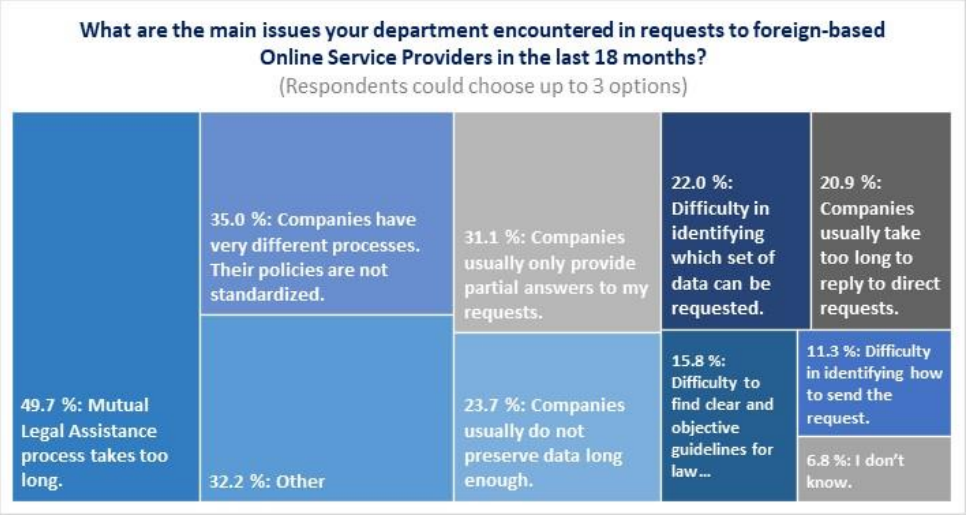




5.2.2. Issues encountered by EU law enforcement

Even if they were mainly satisfied with the process, officers still face a number of challenges in the process to lawfully obtain access to cross-border electronic evidence in the context of criminal investigations. The main issue lies in the fact that MLA processes take too long, according to 49.7 % of respondents. As a matter of fact, the formal process takes around 10 months on average to obtain access to the information[12]. The second issue mentioned by respondents (35%) was the lack of standardization of companies' processes to receive requests from EU law enforcement. In some cases, for example, some very specific vocabulary must be used (e.g. snaps, tweets, stories, etc.) or technical knowledge is required to draft a clear request.

[11] Single Points of Contact (SPOCs) are designated persons, units or institutions who centralize, review and submit requests from governmental authorities to foreign-based OSP. SPOCs may be designated at a LEA or judiciary level and will be responsible for dealing with requests and receiving responses. Some countries may have designated a central unit or authority to act as a SPOC for LEAs or judiciary at a national level.
[12] Daskal, Jennifer, A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right, February 2016.



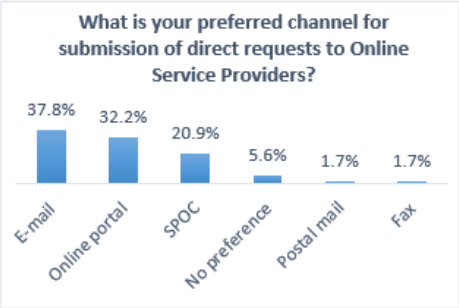
According to 22% of respondents, it is challenging to determine the exact type of data held by companies and therefore to know what could be requested in the context of a criminal investigation. For 15.8% of respondents, it is difficult to find clear and objective guidelines for law enforcement and for 11.3% of them it is difficult to identify how to send requests.

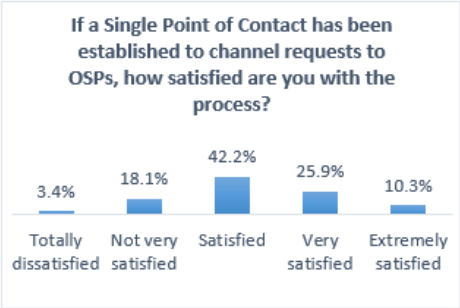
32.2% of respondents pointed out other issues which scored less than 6% each. These other issues are as follows:

- Lack of technological resources to analyse responses;
- Information is only available in English, not in my own language;
- Companies change processes and responses formats too often;
- Requests are usually only accepted in English, not in my own language;
- Companies' responses are not easy to analyse and understand;
- Companies' guidelines are too complicated or too long;
- There are no problems in the process to request digital evidence;
- Other.

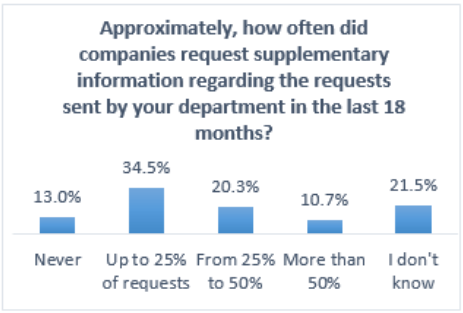
5.2.3. Submission of cross-border requests from EU law enforcement to foreign-based Online Service Providers

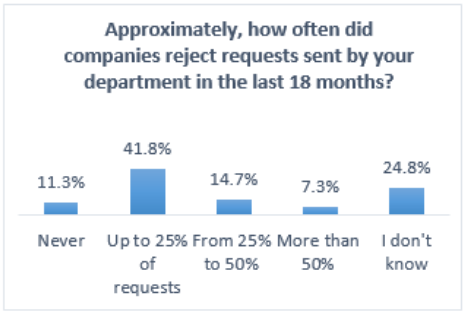
Several OSPs provide dedicated webpages, legal guides and/or restricted online portals for law enforcement and judicial authorities, where they publish information about their processes and requirements. In some cases, it is even possible to submit requests for voluntary cooperation through online portals, as well as follow their status, provide supplementary information and receive the responses securely. For example, Airbnb, Facebook, Uber and WhatsApp have dedicated portals for law enforcement available to all EU Member States. In the EU, 37.8% of respondents prefer to send requests via e-mail, followed by 32.2% who prefer to send via online portals and 20.9% who would rather use SPOCs.



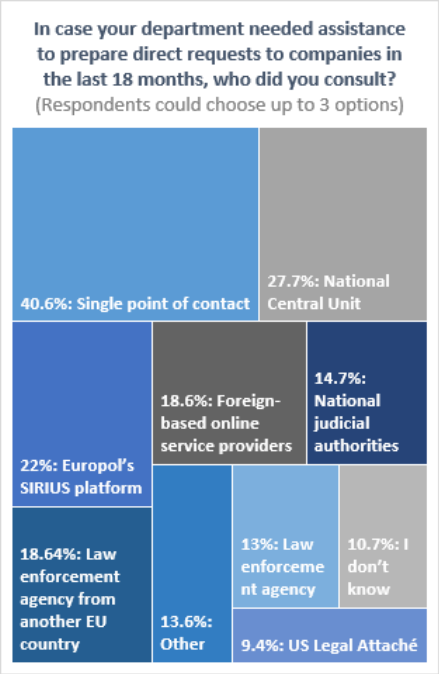


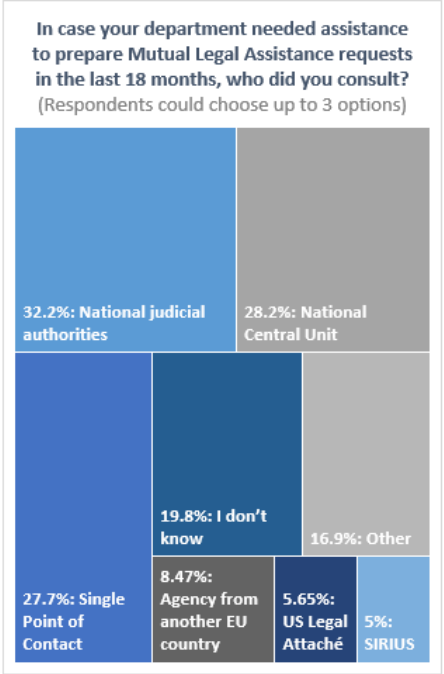
Certain EU LEAs have established Single Points of Contact (SPOCs) within their departments to centralise and submit requests and receive responses from OSPs. Among respondents who work in departments where a SPOC has been established, 78.4% are satisfied, very satisfied or extremely satisfied with the process for the submission of requests. This result could be explained by the fact that the use of SPOCs is generally associated with a higher level of specialization of the submitting officers, who have more experience of working with different companies' processes and requirements.





34.5% of respondents say OSPs requested supplementary information only in the minority of the requests submitted. Regarding the number of rejections by OSPs, 41.8% of respondents say it happened to less than one quarter of the requests.





In the process of submission of direct requests to OSPs, LEAs consulted firstly the SPOC in their departments or in their country (40.6%) and national central units (27.7%). Regarding MLA requests, respondents say they consulted primarily national judicial authorities (32.2%) and national central units (28.2%). Europol's SIRIUS platform was consulted by 22% of respondents for assistance with direct requests to OSPs and by 5% for Mutual Legal Assistance requests.

Respondents were also invited to share success stories of instances where they used electronic evidence in investigations. The success stories below[13] were redacted in part to conceal sensitive information.

- *A serial killer case who killed five women and two under aged girls. There was no other evidence leading to the suspect and the investigators were blind. The [law enforcement agency] was informed about a certain nickname, so a preservation and a request for disclosure of telecommunication data was sent to Facebook and Badoo. They responded immediately and we were finally able to identify the suspect for the murders. This is a recent example of the importance of the retention and disclosure of telecommunication data.*
- *Two threat levels for terrorist attack in [country] were lowered thanks to the emergency disclosure procedure.*
- *In cases of disappearance, murder or attacks, companies such as Apple, Google or Facebook have put in place the appropriate responses and made the necessary efforts to communicate the information to investigators.*
- *Most of the success stories we have are related to emergency disclosure procedures available at some of the largest foreign-based OSPs, including Facebook, Google and Apple. We have used this procedure*

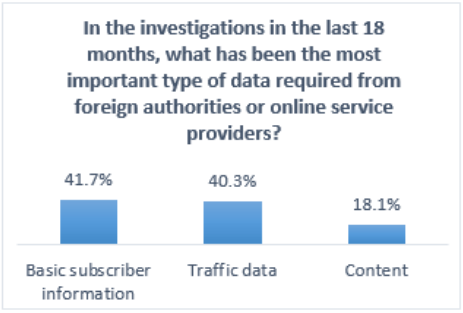
[13] Responses were edited for clarity.

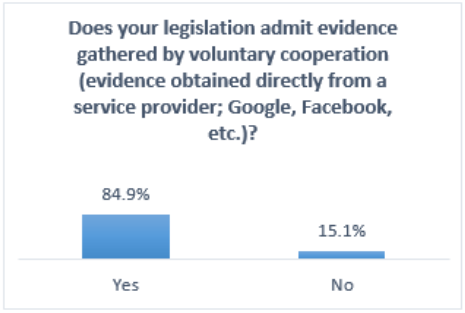
multiple times, especially to investigate missing people cases. Success rate is really high in obtaining necessary information to help proceed with the investigation. Also, emergency disclosure is really quick, so the investigators receive information within 15 to 60 minutes of making the request.

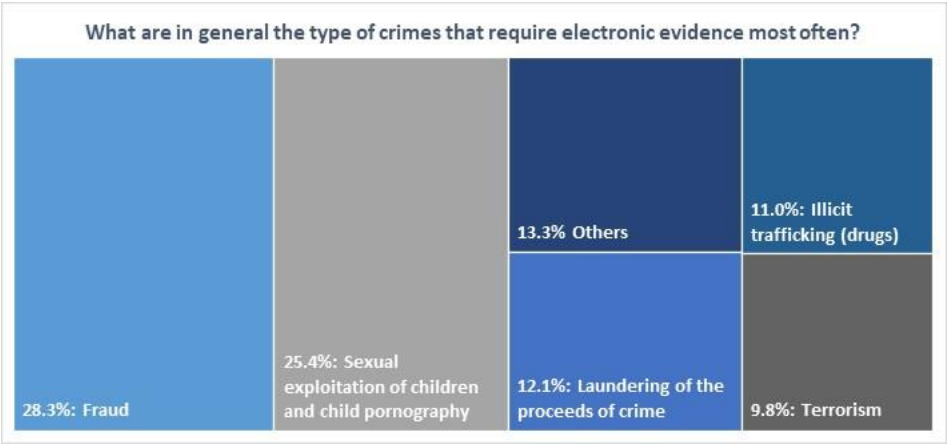
- *We have some good cases, solved mainly by communicating directly with law enforcement from other countries that we met during events such as meetings or conferences, long before the SIRIUS project was established. Now we use data from the SIRIUS project to contact OSPs, and to align our approach with colleagues from other countries*.

5.3 Survey with judicial authorities

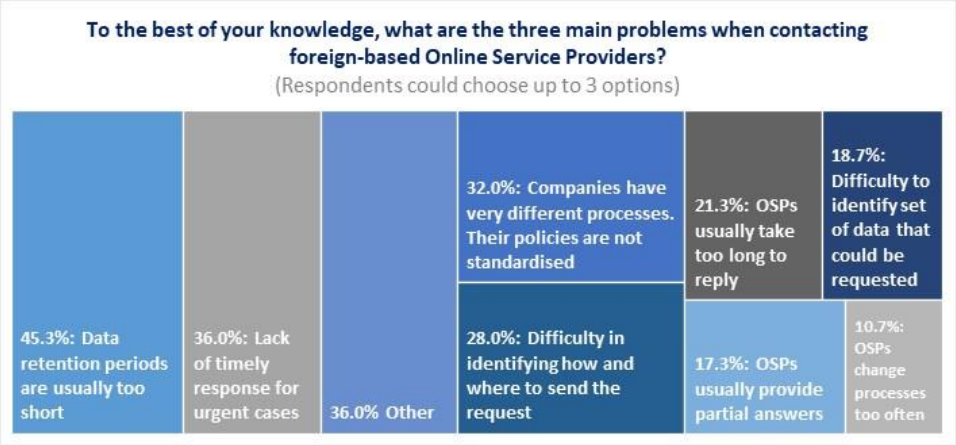
In the majority of investigations, the most needed type of data was Basic Subscriber Information (e.g. name, e-mail, phone number), closely followed by Traffic Data (e.g. connection logs, IP addresses, number of messages), and only then content data (e.g. photos, mail/messages content, files). 84.9% of respondents stated that their national legislation admits evidence gathered by voluntary cooperation with OSPs.





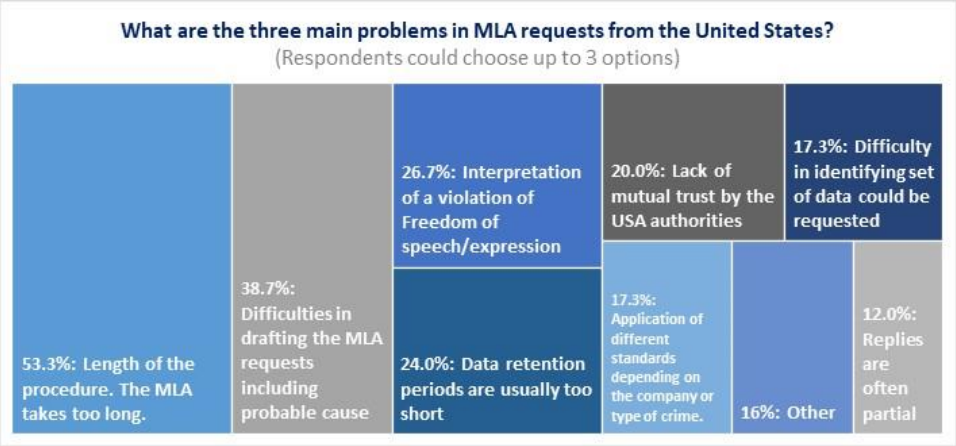


Respondents identified fraud (28.3%) and sexual exploitation of children and child pornography as the main type of crimes that require electronic evidence. 13.3% of respondents identified types of crime that amounted to less than 5% of responses each; the crimes identified in “others” included trafficking in human beings, forgery of means of payment, corruption, rape, illicit trafficking (weapons). No respondent chose the option “trafficking in stolen vehicles”.



Regarding issues in dealing with OSPs, the short data retention period was a problem identified by 45.3% of respondents. 36.0% pointed out the lack of timely response in urgent cases, and 32.0% mentioned that OSP policies are not standardised. 1.3% of respondents stated that there are no problems in the process to request electronic evidence from foreign-based OSPs, and finally, 36.0% identified other issues that scored less than 10% each. These other issues were as follows:

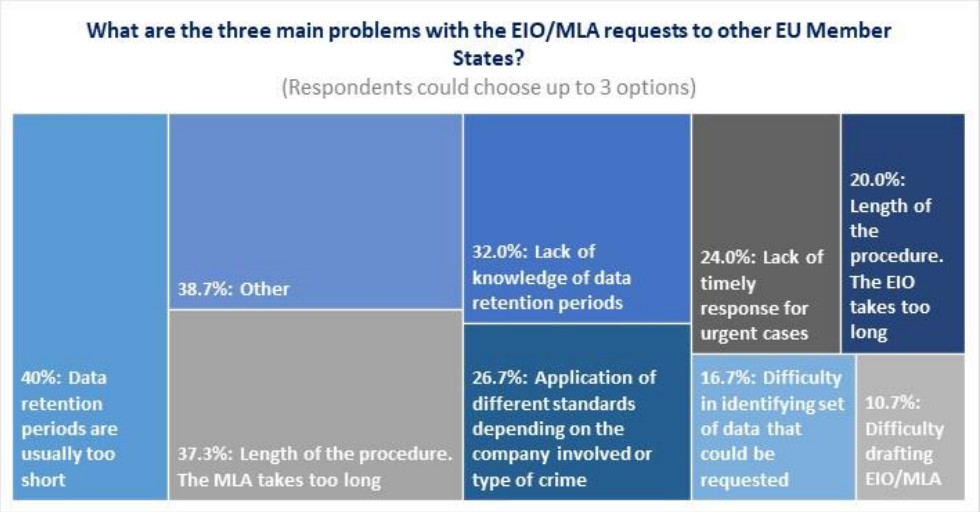
- Lack of trust from the companies towards the requesting country;
- Difficulty to find clear and objective guidelines provided by the company;
- Difficulties with the technical terms used for electronic evidence;
- Companies' guidelines are too complicated or too long;
- Requests are usually only accepted in English, not in my own language;
- My MS lacks the technological resources to analyse responses from service providers;
- Information is only available in English, not in my own language;
- Law enforcement in my country report that companies' responses are not easy to analyse and understand.



When asked about the issues in the MLA request process with the US, 53.3% of respondents identified the long time the procedure takes as the biggest issue. 38.7% of them identified difficulties in drafting the MLA requests including justifying probable cause. 4% of respondents found no issues. Lastly, 16.0% of

them identified other issues that scored less than 10% each. These other issues were as follows:

- Difficulties with the technical terms/language used for electronic evidence;
- Difficulties when contacting/gathering clear instructions by the Department of Justice;
- Difficulties in finding the European Judicial Network Contact Points in the US;
- Information is only available in English, not in my own language.



Regarding the use of the EIO or MLA with other EU MS, 40% of respondents identified the short data retention period as the most serious issue, and 37.3% stated that the MLA process takes too long. 38.7% of respondents provided answers that scored less than 10% each. These other issues were:

- Difficulties with the technical terms/language used for electronic evidence;
- Replies are often partial;
- Difficulties when contacting / gathering clear instructions from the Member States;
- Lack of mutual trust;
- Difficulties to find/get an answer from the European Judicial Network Contact Points;
- Interpretation of a violation of freedom of speech/expression;
- Information is not available in English.

5.4 Interviews with Online Service Providers

5.4.1 Reasons for refusal or delay in processing direct requests for voluntary cooperation from EU authorities

During the interviews conducted with OSPs, it appeared that many of the core issues in processing requests are the same across companies. While it was not

possible to obtain statistical data about specific reasons for refusal, the information provided by OSPs gives a clear indication of what the main issues are, albeit anecdotally. The items are not presented in order of importance.

Wrong identifier provided

Direct requests for voluntary cooperation are often rejected because of non-existent data, as the requesting authority provided invalid identifiers, such as the wrong e-mail addresses, phone numbers, URLs or user name. They could simply be misspelled or be erroneous. Some companies may also refuse requests which only mention the vanity name of the account in question, as vanity names are not necessarily unique on certain platforms and can be changed at any moment by the user, thus increasing the probability of an unreliable response.

Overly broad requests

Requests that would result in the disclosure of a very large number of users' accounts or a very extensive amount of records may be considered excessive. OSPs may also consider as overly broad requests that do not properly justify the need for the data sought. Finally, it is also very common that requests are considered overly broad when requesters ask for "all the data available" regarding the targeted account.

Requests for non-existent data

Rejecting a request for non-existent data can happen for a variety of reasons. Firstly, the requested data could have already been deleted by the users or by the OSP, as some OSPs only keep certain types of data for a specific amount of time. To avoid this situation, it is important to send a preservation request to the company as soon as possible, in accordance with their procedures, to avoid data loss. Secondly, requests can be refused for non-existent data because this is not held by the company. For example, law enforcement might request the profile picture linked to an account, but the user has not uploaded one. Finally, the targeted account might have never existed.

Requests for data that require judicial cooperation

Compliance with direct requests made by authorities to foreign-based companies is voluntary, therefore OSPs may decide to reject the request and instruct the requester to follow judicial cooperation channels. Legislation in certain countries, including the US for example, restrict the voluntary direct disclosure of content data to foreign authorities. Therefore, in situations when law enforcement is requesting content data, OSPs may refuse the request and instruct the requester to follow judicial cooperation channels such as an MLA. Moreover, some companies adopt the policy of only accepting direct requests in emergency circumstances. In these cases, any direct request received from foreign authorities in non-emergency circumstances will be rejected.

Lack of reference to Valid Legal Basis (VLB) for direct requests under the domestic legislation of the requesting authority

Since responses to direct requests are provided on a voluntary basis, OSPs may set their own policies and requirements. In this context, some OSPs require the

foreign requesting authority to state the legal basis for such request under their domestic legislation. As a consequence, these companies may reject requests that do not include VLB.

Requests addressed to the wrong legal entity

OSPs often have legal entities and servers in different countries. Requests for the disclosure of users' data should be submitted in accordance with the applicable regulations for the legal entity which is the data controller.

Lack of preservation request and wrong process for extension of preservation requests

When OSPs process preservation requests, they usually provide a response to the requesting authority informing them of the period during which the data is going to be preserved, as well as an internal reference code, which should be used in all related requests.

Some of the most common rejection reasons related to preservation requests are:

- The data no longer exists, as no preservation request was made;
- The data disclosure request is served after the expiration of the preservation period;
- The data disclosure request did not mention that a previous preservation request had been made or the reference number provided by the company after processing a preservation request;
- The authority followed the wrong process for an extension: it is necessary to request an extension of the data preservation by following the processes described in the companies' policies, and not by issuing a new preservation request. If authorities issue a new preservation request, the company will capture the data at the time of the new request, which may not include the data preserved in the original preservation request.

5.4.2 Challenges from the perspective of Online Service Providers

Online Service Providers dealing with incoming requests directly from foreign-based law enforcement and judicial authorities also face a number of challenges. One of the issues mentioned by representatives of the companies is the language barrier. Maintaining full time capacity to deal with requests in several languages requires significant resources which are not always available, especially for smaller OSPs. Most of the companies require direct requests to be submitted in English, or to include a translation in English. Requests submitted in other languages may require a longer processing time.

Another issue is to ensure the documents received are authentic and submitted by an authorised official. Most companies rely on the governmental domain of e-mail addresses of requesters. Many MS have multiple governmental domains, depending on the authority or the agency, which cannot always be easily authenticated. Furthermore, the fact that someone has a governmental e-mail address not always necessarily means that person is

an authorised official. To overcome this issue, companies rely on the information, stamp and signatures provided in the attached request or legal process.

Some OSPs also mentioned the challenge of evaluating whether a request corresponds to an emergency as defined by the applicable legislation, when very little context is provided by the requester. In some instances, it is necessary to request supplementary information from foreign-based authorities to ensure the case falls into that category. Since companies make their own assessments in emergencies, it is important that requests include as much background information as possible, so as to justify the need for the disclosure of data without delay.

Finally, many OSPs insist that a large number of the misunderstandings during the data request process stem from requesters having little or no previous knowledge of their services and products. In several instances, representatives from companies advise authorities to use their services to familiarise themselves with their functionalities. Being aware of how the platforms operate and how the users interact with them could facilitate drafting clearer and more objective requests.

6. Recommendations

This report focused on the situation of cross-border requests for electronic evidence in 2018. The information gathered gives indications of short-term actions which could be taken to improve the swiftness of this process. The recommendations in this session are directed to OSP and LEAs and may be applicable regardless of potential future developments in policy and regulations.

6.1 Recommendations to Online Service Providers

Provide clear guidelines for law enforcement authorities, including information about which data sets can be requested and to which legal entity the data requests should be addressed

Most of the biggest OSPs have publicly available guidelines for law enforcement. These documents contain essential information for authorities seeking data in the context of criminal investigations. Since each company may have different policies regarding direct requests from foreign-based authorities, publicly available guidelines play a key role in expediting investigations and are especially important in time-sensitive and life-threatening cases. It is recommended that these documents include a list of the data sets that can be requested by authorities, which would limit overly broad requests. Moreover, it is important to state which legal entity is the data controller, which will avoid delays and unnecessary requests.

Prepare periodic transparency reports regarding requests from EU authorities, including standardised data categories across Online Service Providers and files in CSV formats

Transparency reports are extremely important from an analytical perspective, as they give a clearer picture of cross-border access to electronic evidence, identify trends and common issues, and better inform authorities of which mistakes to avoid. Since products and services from OSPs vary widely, it is understandable that transparency reports will reflect this variety and include each company's specific information. However, in order to properly analyse the data, a minimum standardisation level is highly recommended. The SIRIUS project recommends that companies publish transparency reports in editable format (e.g. .csv) at least yearly, distinguish civil from criminal cases and include at a minimum the following **breakdown of data per country**:

- Total number of requests;
- Number of accounts concerned by requests;
- Disclosure rate of all types of requests;
- Total number of emergency requests;
- Number of accounts concerned by emergency requests;

- Disclosure rate of emergency requests;
- Total number of preservation requests.

In case of rejection of direct requests or emergency disclosure requests, clearly inform the requesting authority of the reasons for rejection without delay

It is crucial for law enforcement and judicial authorities to know the reasons why companies could not comply with a request. This information will allow the requesting authority to determine whether to submit a new request, provide supplementary information or simply pursue different investigative paths.

6.2 For European Union Law Enforcement Agencies

Provide periodic trainings to officers dealing with cross-border requests to Online Service Providers

In the survey conducted by Europol for the purpose of this report, 49% of law enforcement officers reported never having received training regarding how and when to make cross-border requests to OSPs. 32% reported receiving such trainings less often than every two years. In a fast evolving digital world, it is crucial to receive periodic trainings regarding electronic evidence, which can increase the effectiveness and the speed of investigations. This is particularly important when dealing with emergency situations and time-sensitive cases.

The SIRIUS platform makes available material and e-learning modules on cross-border access to electronic evidence, which are accessible to all EU law enforcement agencies.

In Member States where there is no central unit for submission of requests, establish Single Points of Contact within the law enforcement agency to deal with the most relevant Online Service Providers

Creating a process for submission of requests to OSPs via one or more designated point(s) of contact has a number of benefits. For instance, it allows for a higher level of specialisation and thus contributes to faster and smoother processes of cross-border data requests. Officers who submit requests regularly are more familiar with the vocabulary to use, what data may be requested in each situation, what information must be provided in the request, as well as how to submit the requests to the companies (e.g. via e-mail, online portals, fax). The creation of SPOCs also allows for the collection of centralised statistics and facilitates the dissemination of updates from the companies, including new products and services.

Most of the major OSPs welcome the creation of SPOCs, as it also facilitates the authentication of incoming requests and increases their quality. In the survey among EU LEAs, 64% reported being satisfied, very satisfied or extremely satisfied with their SPOC.

Collect statistics regarding cross-border requests to Online Service Providers

The collection of statistics regarding requests to OSPs may be useful internally within LEAs in order to identify trends in the abuse of these services by criminals and thus increase law enforcement's capacity to tackle them. It may also be of interest in order to identify priority areas for training and investigative resources.

7. References

Agreement on mutual legal assistance between the European Union and the United States of America, Official Journal L 181, 19/07/2003 P. 0034 – 0042, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:22003A0719(02)

Airbnb Supplemental Law Enforcement Transparency Reports, available at: https://www.airbnbcitizen.com/transparency

Apple Transparency Report, available at: https://www.apple.com/legal/transparency/

Automattic Information Requests, available at: https://transparency.automattic.com/information-requests/

Cloudflare transparency report, available at: https://www.cloudflare.com/transparency/

Convention on Cybercrime ETS No.185, Budapest, 23/11/2001, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Council gives mandate to Commission to negotiate international agreements on e-evidence in criminal matters, Council of the European Union, Press release 06/06/2019, available at: https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

Daskal, Jennifer, A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right, February 2016.

E-evidence, DG Migration and Home Affairs, available at: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en

Facebook Transparency Government Requests for User Data, available at: https://transparency.facebook.com/government-data-requests

Google Transparency Report, requests for user information, available at: https://transparencyreport.google.com/user-data/overview?hl=en

Impact assessment - e-Evidence - the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, European Commission, April 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN

Linkedin Transparency Report, available at: https://www.linkedin.com/legal/transparency

Microsoft Law Enforcement Requests Report, available at: https://www.microsoft.com/en-us/corporate-responsibility/lerr

Oath Transparency Report, available at: https://transparency.oath.com

Regulation on cross-border access to e-evidence: Council agrees its position, Council of the European Union, Press release 07/12/2018, available at: https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/

Snap Inc. Transparency Report, available at: https://www.snap.com/en-US/privacy/transparency/

Transparency at Dropbox, available at: https://www.dropbox.com/en_GB/transparency/reports

Twitter Transparency Report – Information Requests, available at: https://transparency.twitter.com/en/information-requests.html

All links were last accessed on: 08/10/2019

Annex 1 – Survey with EU law enforcement agencies

1. On a scale from 1 to 5, how satisfied are you with your department's engagement with foreign-based Online Service Providers in the last 18 months?

- 1 Totally dissatisfied
- 2 Not very satisfied
- 3 Satisfied
- 4 Very satisfied
- 5 Extremely satisfied

2. In the majority of the investigations in the last 18 months, what is the most important type of data your department needed?

- Basic subscriber information (e.g. name, e-mail, phone number)
- Traffic data (e.g. connection logs, IP addresses, number of messages)
- Content (e.g. photos, mail/messages content, files)
- I don’t know.

3. What type of request to Online Service Providers was used the most by your department in the last 18 months?

- Direct requests
- Emergency disclosure requests
- Mutual Legal Assistance requests
- European Investigation Order
- I don't know

4. How often do you receive training regarding cross-border requests for electronic evidence?

- Twice a year or more
- Yearly
- Every two years
- Less often than every two years
- Never

5. What is your preferred channel for submission of direct requests to Online Service Providers?

- E-mail

- Postal mail
- Online portal
- Fax
- Single Point of Contact in my department or in my country
- I don’t have a preference

6. Approximately, how often did companies request supplementary information regarding the requests sent by your department in the last 18 months?

- Never
- Up to 25% of requests
- From 25% to 50% of requests
- More than 50% of requests
- I don't know

7. In case your department needed assistance to prepare direct requests to companies in the last 18 months, who did you consult?

- National Central Unit
- Single Point of Contact in my country
- Other national law enforcement agency
- Law enforcement agency from another EU country
- Law enforcement agency from a non-EU country
- Foreign-based Online Service Providers
- National judicial authorities
- Europol’s SIRIUS platform
- US Department of Justice
- US Legal Attaché in my country
- US Embassy
- I don’t know
- Other

8. In case your department needed assistance to prepare Mutual Legal Assistance requests in the last 18 months, who did you consult?

- National Central Unit
- Single Point of Contact in my country
- Other national law enforcement agency
- Law enforcement agency from another EU country
- Law enforcement agency from a non-EU country
- Foreign-based Online Service Providers
- National judicial authorities
- Europol’s SIRIUS platform
- US Department of Justice
- US Legal Attaché in my country
- US Embassy
- I don’t know
- Other

9. What are the main issues your department encountered in requests to foreign-based Online Service Providers in the last 18 months?

- Difficulty in identifying which set of data can be requested from companies.
- Difficulty to find clear and objective guidelines for law enforcement.
- Companies change processes and responses formats too often.
- Companies usually take too long to reply to direct requests.
- Companies' guidelines are too complicated or too long.
- Information is only available in English, not in my own language.
- Difficulty in identifying how to send the request.
- Requests are usually only accepted in English, not in my own language.
- Mutual Legal Assistance process takes too long.
- Companies have very different processes. Their policies are not standardized.
- Companies usually do not preserve data long enough.
- Companies usually only provide partial answers to my requests.
- Companies' responses are not easy to analyse and understand.
- Lack of technological resources to analyse responses from service providers.
- There are no problems in the process to request digital evidence.
- I don't know.
- Other

10. Approximately, how often did companies reject requests sent by your department in the last 18 months?

- Never
- Up to 25% of the requests
- From 25% to 50% of the requests
- More than 50% or the requests
- I don't know

11. Has your department (or your country) established a Single Point of Contact to channel requests to one or more foreign-based companies?

- Yes
- No
- I don't know

12. If a Single Point of Contact has been established to channel requests to one or more foreign-based companies, how satisfied are you with the process?

- 1 Totally dissatisfied
- 2 Not very satisfied
- 3 Satisfied
- 4 Very satisfied
- 5 Extremely satisfied
- Not applicable

13. What were the three most relevant Online Service Providers in your department's investigations in the last 18 months?

14. What are the three Online Service Providers with which you have encountered the most issues when requesting data in the last 18 months?

15. What are common reasons companies give when they reject requests sent by your department?

16. How do you evaluate the current process to lawfully request data disclosure from foreign-based Online Service Providers?

17. Share a success story. We are interested to hear about example of cases in which electronic evidence obtained through Direct Request or MLA was essential in investigations. If you used the SIRIUS platform, let us know. (ATTENTION: DO NOT SHARE OPERATIONAL DATA OR PERSONAL INFORMATION HERE.)

Annex 2 – Survey with EU judicial authorities

1. In the investigations in the last 18 months, what has been the most important type of data required from foreign authorities or Online Service Providers?

- Basic subscriber information (e.g. name, e-mail, phone number)
- Traffic data (e.g. connection logs, IP addresses, number of messages)
- Content (e.g. photos, mail/messages content, files)

2. What are in general the type of crimes that require electronic evidence most often? Investigations that require electronic evidence for the following crimes:

- terrorism
- trafficking in human beings
- sexual exploitation of children and child pornography
- illicit trafficking (drugs)
- illicit trafficking (weapons)
- corruption
- fraud
- laundering of the proceeds of crime
- forgery of means of payment
- trafficking in stolen vehicles
- rape

3. Computer dependent crime (cybercrime)

- Crimes specific to the Internet, such as attacks against information systems or phishing (e.g. fake bank websites to solicit passwords enabling access to victims' bank accounts).
- Online fraud and forgery. Large-scale fraud can be committed online through instruments such as identity theft, phishing, spam and malicious code.
- Illegal online content, including child sexual abuse material, incitement to hate crimes, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia.

4. Does your legislation admit evidence gathered by voluntary cooperation (evidence obtained directly from a service provider; Google, Facebook, etc.)?

- Yes
- No

5. To the best of your knowledge, what are the three main problems when contacting foreign-based Online Service Providers?

- Difficulty in identifying set of data that could be requested from companies
- Difficulty to find clear and objective guidelines provided by the company
- Companies' guidelines are too complicated or too long
- Lack of timely response for urgent cases
- Companies change processes and responses formats too often
- Companies usually take too long to reply to direct requests
- Lack of trust by the companies on the requesting State
- Difficulties with the technical terms used for electronic evidence
- Information is only available in English, not in my own language
- Information is not available in English
- Difficulty in identifying how and where to send the request
- Requests are usually only accepted in English, not in my own language
- Requests are not accepted in English
- Companies have very different processes. Their policies are not standardised
- Data retention periods are usually too short
- Companies usually only provide partial answers to my requests
- Law enforcement in my country report that companies' responses are not easy to analyse and understand
- My Member State lacks the technological resources to analyse responses from service providers
  or
- There are no problems in the process to request electronic evidence

6. What are the three main problems in MLA requests from the United States:

- Difficulties when contacting / gathering clear instructions by the Department of Justice

- Difficulties to find the EJN Contact Points in the USA
- Lack of mutual trust by the USA authorities
- Interpretation of a violation of Freedom of speech/expression
- Difficulties in drafting the MLA requests including probable cause
- Difficulty in identifying set of data could be requested
- Data retention periods are usually too short
- Difficulties with the technical terms/language used for electronic evidence
- Information is only available in English, not in my own language
- Application of different standards depending on the company involved or type of crime. Their policies are not standardized
- Length of the procedure. The MLA takes too long
- Replies are often partial
  or
- There are no problems in the process to request electronic evidence

7. What are the three main problems with the EIO/MLA requests to other EU Member States:

- Difficulties when contacting / gathering clear instructions from the Member States
- Difficulties to find/get an answer from the EJN Contact Points
- Lack of mutual trust
- Lack of timely response for urgent cases
- Interpretation of a violation of Freedom of speech/expression
- Difficulties in drafting the EIO/MLA requests
- Difficulty in identifying set of data that could be requested
- Data retention periods are usually too short
- Lack of knowledge of data retention periods
- Difficulties with the technical terms/language used for electronic evidence
- Information is only available in English, not in my own language
- Information is not available in English
- Application of different standards depending on the company involved or type of crime. Their policies are not standardised
- Length of the procedure. The MLA takes too long
- Length of the procedure. The EIO takes too long
- Replies are often partial
  or
- There are no problems in the process to request electronic evidence

8. What works well when requiring electronic evidence to the United States (or from other countries)?

9. What are the three Online Service Providers with which you have encountered more issues when requesting data in the last 18 months?

10. What were the three most relevant Online Service Providers in your cases in the last 18 months?

11. The Commission has proposed a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters which is meant to make it easier and faster to obtain the electronic evidence. Considering that this proposal aims to: create a European Production order: this will allow a judicial authority in one Member State to obtain electronic evidence (such as emails, text or messages in apps, as well as information to identify a perpetrator as a first step) directly from a service provider or its legal representative in another Member State, which should respond within 10 days, and within 6 hours in cases of emergency); create a European Preservation Order: this will allow a judicial authority in one Member State to request that a service provider or its legal representative in another Member State preserves specific data in view of a subsequent request to produce this data via Mutual Legal Assistance, a European Investigation Order or a European Production Order; (For further information please see the new section of the EJN website on e-Evidence) Do you think that European Production and Preservation Orders Regulation would improve the current situation? Why? Why not?

12. Which are the biggest challenges that you are able to identify in applying the Regulation in practice?

13. Any other comments?