SIRIUS EU DIGITAL EVIDENCE SITUATION REPORT

20 DECEMBER 2019

MANAGEMENT SUMMARY

The SIRIUS EU Digital Evidence Situation Report 2019 intends to draw a picture of the status of access of EU Member States (MS) to electronic evidence held by foreign-based Online Service Providers (OSPs) in 2018. The report presents data in relation to the volume of requests from EU MS to OSPs, the main reasons for refusal or delay of EU requests and the main challenges in the process, from the perspective of the different stakeholders. The report is mainly analytical and does not propose conclusions. Instead, it contains practical recommendations to OSPs and LEAs which could improve the process for requests to e-evidence.

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 the e-evidence is located, or where the service provider exploited is, are all in different countries. 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 child sexual exploitation, human trafficking and terrorism.

At present, there are different ways to request lawful cross-border access to data held by OSPs in the content of criminal investigations. Legislation in this regard varies from country to country and different international legal instruments may be applicable. The processes of requests from government authorities to private companies also vary according to the type of data sought and how sensitive it is.

MAIN FINDINGS

From EU law enforcement and judicial authorities:

- 49% of LE officers never received proper training about cross-border access to e-evidence.
- Even if EU law enforcement is mainly satisfied with the processes in obtaining e-evidence, officers still face a number of challenges in lawfully obtaining access to cross-border e-evidence in the context of criminal investigations.
- The main issue lies in the fact that MLA processes take too long. Currently, the formal process to obtain e-evidence via MLA to the United States takes around 10 months on average.
- The second issue is the lack of standardisation of companies' processes to receive requests from EU law enforcement.
- Other issues include: challenges in determining the exact type of data held by companies; difficulties in finding clear and objective guidelines for law enforcement; and difficulties in identifying how to send requests.
- Certain EU law enforcement authorities have established Single Points of Contact (SPOC) within their departments to centralise and submit requests and receive responses from OSPs. Among respondents who use SPOCs, 78% reported being satisfied, very satisfied or extremely satisfied with their SPOC.
- Judicial authorities highlighted the length of the MLA process and the difficulty in meeting probable cause standard as the main problems in requests to the US. They appointed the short data retention periods as the main issue in requests to other Member States.
- 22% of law enforcement respondents say they use Europol's SIRIUS Platform for assistance in drafting direct requests to OSPs; 5% use it for drafting MLA requests.

From OSPs:

- Success rate of EU requests to eight major OSPs in 2018 was 66%.
- The OSPs usually carry out an internal review of the requests based on their own definitions. For example, Twitter states that it rejects requests that are "improper" which it defines as including "invalid or overly broad legal process".
- Reasons OSPs refuse or delay requests: wrong identifier provided; overly broad requests; requests for non-existent data; requests for data that require judicial cooperation; lack of reference to Valid Legal Basis for direct requests under the domestic legislation of the requesting authority; requests addressed to the wrong legal entity; and lack of preservation request and wrong process for extension of preservation request.
- One of the main challenges for companies dealing with foreign-based law enforcement and judicial authorities is the language barrier.
- Another issue is to ensure documents received are authentic and submitted by an authorised official.
- Some OSPs find evaluating whether a request corresponds to an emergency as defined by the applicable legislation challenging, when very little context is provided by the requestor.
- Many OSPs insist that a large number of the misunderstandings during the data request stem from requesters having little or no previous knowledge of their services and products.

RECOMMENDATIONS

To OSPs:

- 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.
- Prepare periodic transparency reports regarding requests from EU authorities, including standardised data categories across OSPs and files in CSV formats.
- In case of rejection of direct requests or emergency disclosure requests, clearly inform the requesting authorities of the reasons for rejection without delay. This information is important because it allows the requesting authority to determine whether to submit a new request, provide supplementary information or simply pursue different investigative paths.

To EU law enforcement authorities:

- Provide periodic trainings to officers dealing with cross-border requests to OSPs.
- Establish Single Points of Contact within law enforcement to deal with the most relevant OSPs.
- Collect statistics regarding cross-border requests to OSPs. This may be useful in identifying trends in abuse of these services by criminals and may be of interest to identify priority areas for training and investigative resources.

Report published at: https://www.europol.europa.eu/newsroom/news/sirius-european-union-digital-evidence-situation-report-2019