First EU Digital Evidence Situation Report Published

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle
Deputy Head of Section
Academy of European Law

ISSN: 1862-6947
https://eucrim.eu

On 20 December 2019, Europol published a new report, giving an overview on the status of access of EU Member States to electronic evidence held by foreign-based Online Service Providers (OSPs) in the context of criminal investigations. Looking at the year 2018, the new EU Digital Evidence Situation Report (SIRIUS) looks at the volume of requests from EU Member States to OSPs, the main reasons for refusal or delay of EU requests, and the main challenges in the process.

According to the report, over 74% of EU law enforcement requests to the eight major OSPs in 2018 originated in three EU Member States: Germany, France, and the UK. The three OSPs most frequently requested were Facebook (30%), Google (26%), and Apple (24%). The overall success rate of requests to major OSPs in 2018 was calculated at 66%. The most frequently needed type of data in the majority of investigations appeared to be traffic data (e.g., connection logs, IP addresses, number of messages), followed by basic subscriber information (e.g., name, e-mail, phone number), and content data (e.g., photos, mail/message content, files).

Looking at issues encountered by EU law enforcement, with requesting data from OSPs, the main problems identified by the report are the lengthy MLA proceedings, the lack of standardized company procedures when receive requests from EU law enforcement, and how to determine the type of data held by companies. Further issues outlined in the report include the short data retention period, the lack of timely response in urgent cases, and the non-standardization of OSP policies.

Reasons for refusal or delay in processing direct requests, as given by the OSPs, include wrong identifiers, overly broad requests, requests concerning non-existing data or data requiring judicial cooperation, the lack of reference to Valid Legal Basis (VLB) under the domestic legislation of the requesting authority, the wrong legal entity of the OSP being addressed, and the lack of requests for preservation. Other challenges faced by the OSPs are language barriers, how to ensure the authenticity of received documents, and misunderstandings caused by little or no previous knowledge on the part of requesters of OSP services and products.

The report provides for several recommendations to both the OSPs and EU law enforcement agencies. OSPs are asked to 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; to prepare periodic transparency reports on requests from EU authorities, including standardized data categories across OSPs and files in CSV formats; and to clearly inform the requesting authority of the reasons for rejection without delay. EU law enforcement agencies are asked to provide periodic trainings to officers dealing with cross-border requests to OSPs; to establish Points of Single Contact (PSCs) within the law enforcement agency to deal with the most relevant OSPs; and to collect statistics on cross-border requests to OSPs.

The report is an outcome of the SIRIUS project, which was launched by Europol in October 2017. The project was initiated in response to the increasing need of the EU law enforcement community to access electronic evidence for internet-based investigations. More than half of all criminal investigations today include a cross-border request to access e-evidence (such as texts, e-mails, or messaging apps). The SIRIUS project is spearheaded by Europol's European Counter-Terrorism Centre and European Cybercrime Centre, in close partnership with Eurojust and the European Judicial Network. It aims to help investigators cope with the complexity and volume of information in a rapidly changing online environment, by providing guidelines on specific OSPs and investigative tools. Europol established a platform for experts (restricted access) by means of which the multidisciplinary SIRIUS community can have access to a wide range of resources.

The EU Digital Evidence Situation Report provides empirical information on e-evidence in a systematic and comprehensive way for the first time. It not only includes information from all EU Member States but also comprises data from both judicial and police authorities. Another added value is the input by 12 OSPs (mainly based in the USA, e.g., Airbnb, Facebook, Google, Microsoft, Twitter). The report is sure to influence discussion on the establishment of a new legal framework on e-evidence at the EU level (see, recently, eucrim 3/2019, pp. 179 et seq. with further references).

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union