Council of the European Union
General Secretariat

Brussels, 11 May 2017

DOCUMENT PARTIALLY ACCESSIBLE
TO THE PUBLIC (12.01.2018)

WK 5380/2017 INIT

LIMITE

JAI
COPEN
DAPIX
ENFOPOL
CYBER

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Europol
To:	DAPIX (Friends of the Presidency - Data Retention)
Subject:	Data categories to be retained for law enforcement purposes

Council Working Party on Information Exchange and Data Protection (DAPIX) Friends of Presidency

The Hague, 11 May 2017

EDOC# 895573v8

Data categories to be retained for law enforcement purposes

DAPIX Friends of Presidency meeting 15 May 2017, Brussels

Europol contribution

1. Background

Referring to Europol's contribution to the Council Working Party on General Matters including Evaluation (GENVAL) discussion of 3 February 2017 "Retention of electronic communication data: Problem statement"[1] and the contribution to the Council Working Party on Information Exchange and Data Protection (DAPIX) Friends of Presidency following the discussion of 10 April 2017 "Cases affected by the current data retention regime"[2], this document **outlines scenarios that require different data categories to be retained for law enforcement (LE) purposes in the context of an investigation with the ultimate aim of attribution of criminal activity to an individual perpetrator.**

1.1. Threat picture

Technological innovation continues to shape society and the economy, and by extension the serious and organised crime landscape in Europe. Criminal actors in the EU and beyond display a high degree of adaptability, creativity and entrepreneurship in exploiting and employing new technologies for criminal activity. While not all criminal activities are driven by technological developments, the internet and ever-increasing connectivity have an impact on virtually all types of serious and organised crime as well as terrorism, despite the many undeniably positive effects and opportunities the internet creates.

Innovation in technology is increasingly being abused by Organised Crime Groups and terrorists to commit crime anonymously, anywhere and anytime without having to be physically present to attack their victims. The Internet of Things is constantly expanding. Connectivity of all types of devices, including phones and appliances, is increasingly a reality in households and businesses across the EU.[3] This introduces additional vulnerabilities, which combined with the development of a service-based economy that facilitates low-risk, low-cost, and high-profit cyber criminality at a global scale, further exacerbates the threat.

This expanding Crime-as-a-Service business model provides a wide range of services that allow criminals to hide their intentions, hide their location, obscure their identity and obfuscate their financial transactions. This renders it considerably more difficult for law enforcement to retrieve relevant electronic data that can be used as judicial evidence, in particular when such data is located in third countries.

---

[1] EDOC# 881338v11

[2] EDOC# 892624v5

[3] Europol Serious and Organised Crime Threat Assessment 2017 – Crime in the age of technology; https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

1.2. Law enforcement response

Today, electronic data such as IP addresses often are the starting point of an investigation, meaning that the necessary data and potential evidence is born digitally. Such cases cannot necessarily be solved through “classic police work” or investing more resources.

For instance, in a high-value counterterrorism propaganda case supported by the EU Internet Referral Unit at Europol, more than 2,000 IP connections in 19 different EU Member States could not be traced back to suspects at large because the IP log files containing the relevant information were no longer stored by the respective internet service providers (ISP).

In the event of an investigation into organised crime or a terrorist attack, investigators try to identify the victims, the (deceased) perpetrators/suspects, and potential suspects at large. **Critical success factors** include (1) the urgency of retrieving relevant information as another attack or crime may be imminent, (2) the accuracy of the data retained with a view to properly targeting the investigation in a short timeframe, (3) to separate the wheat from the chaff, also referred to as noise reduction: instead of collecting mass data, LE needs the capability to identify and extract relevant information in larger data collections. Forensic analysis to extract relevant data can be time and resource intensive, particularly if the data is encrypted or if the number of requests has to be multiplied by the number of devices, providers and countries involved, and when International Letters of Rogatory have to be submitted via the judiciary and diplomatic channels.

2. Use cases

DELETED

3. Conclusion

Europol argues against a ranking of data categories according to their importance as operational experience has shown that investigations start with the data that is available for a particular crime. The available data will be considered the most relevant one, and may differ from case to case. As shown by the examples above this could be an IP address, a telephone number, an online nickname, a social media account or a Bitcoin wallet.

With this in mind, different levels of threshold might apply to different categories of data depending on the level of interference into personal rights of the suspects, victims, and possibly non-involved others. Such approach would mirror the varying levels of authorisation required in traditional investigations, e.g. police subpoena vs. magistrate or prosecutor's prerogative.

--- o ---

DELETED FROM THIS POINT UNTIL THE END OF THE DOCUMENT (page 7)