OCTOPUS CONFERENCE
Strasbourg, 20-22 November 2019

Workshop 2: data protection and criminal justice: what are the issues

Conditions for obtaining subscriber information in relation to dynamic versus static IP addresses

Summary of a T-CY discussion paper (October 2018)

Alexander Seger
Head of Cybercrime Division
Council of Europe

www.coe.int/cybercrime

1

Background

Cybercrime Convention Committee ▶Cloud Evidence Group (2016)

- Subscriber information most often required in criminal investigations. Often starting point of an investigation.
- Less privacy-sensitive than traffic or content data. Rules for access to subscriber information not harmonised.
- Subscriber information held by service providers and obtained through production orders. Lesser interference in rights than search and seizure.

Field	Value
Login (account)	John.doe@gohoo.com
First Name	John
Last Name	Doe
State	Alsace
Zip	67000
Country	France
Timezone	GMT +1
Registered from	IP 194.59.24x.xx
Date Registered	10/01/2016 1:05:18 PM
Last Login	IP 192.60.xxx.xx

2

Background

Cybercrime Convention Committee ▶Cloud Evidence Group (2016)

- **Subscriber information most often required in criminal investigations. Often starting point of an investigation.**
- **Less privacy-sensitive than traffic or content data. Rules for access to subscriber information not harmonised.**
- **Subscriber information held by service providers and obtained through production orders. Lesser interference in rights than search and seizure.**

Solutions proposed

- **Guidance Note on Article 18 (production orders with respect to subscriber information)**
- **Domestic powers according to Article 18**
- **Additional solutions in a Protocol to the Budapest Convention**

3

The issue

- **Additional solutions on obtaining subscriber information through direct cooperation with service providers or expedited international cooperation are to be developed in the Protocol to the Budapest Convention.**
- **However, several court decisions regarding the nature of subscriber information in relation to dynamic as opposed to static IP addresses.**

▶ **Should subscriber information related to dynamic IP addresses be considered (equivalent to) traffic data, and thus would rules for obtaining traffic data (and not rules for obtaining subscriber information) apply to dynamic IP addresses?**

4

The issue

In short:

If production of such data is ordered in a specific criminal investigation, does it make a difference if these are static or dynamic IP addresses? Are different rights affected?

Field	Value
Login (account)	John.doe@gohoo.com
First Name	John
Last Name	Doe
State	Alsace
Zip	67000
Country	France
Timezone	GMT +1
Registered from	IP 194.59.24x.xx
Date Registered	10/01/2016 1:05:18 PM
Last Login	IP 192.60.xxx.xx

5

Relevant court decisions and developments

- German Federal Constitutional Court (2012): Access to subscriber information under the Telecommunications Act
- Supreme Court of Canada (2014): Spencer
- Court of Justice of the European Union (2014 and 2016): Data retention decisions
- Constitutional Court of Portugal (2017): judgment no. 420/2017 on the retention of subscriber information
- European Court of Human Rights (2018): Benedik versus Slovenia
- Court of Justice of the European Union (2018): Case C-207/16 Ministerio Fiscal
- Proposal for an EU Regulation on European Production and Preservation Orders

6

Consideration 1

The purpose of obtaining subscriber information in a criminal justice context:

- To identify the subscriber of a specific account or website, or the subscriber of an IP address in relation to a specific criminal investigation.
- To reconstruct the link between a subscriber and a concrete communication, or vice versa.

Subscriber information as such does not permit precise conclusions to be drawn in respect of the private lives of individuals.

The retention and production of subscriber information as such is unlikely to interfere with the right to the secrecy of communications, although it is likely to interfere with other rights.

7

Consideration 2

The disclosure of subscriber information in specific criminal investigations, in principle, represents a less serious interference with the rights of individuals, including rights to the secrecy of communication or to informational self-determination, than the disclosure of traffic or content data.

- Some Parties ► Lower threshold for disclosure
- Some Parties ► Depends on context, case by case

8

Consideration 3

- Access to subscriber information in specific criminal investigations below the threshold of "serious crime" needed. Seriousness not always known at outset.
- Limiting access to or disclosure of subscriber information to investigations of serious crime would prevent governments from meeting their obligations to protect individuals and their rights against crime.

Court of Justice of the European Union (2018): Case C-207/16 Ministerio Fiscal

Question of whether access to subscriber information – here to identify users of telephone numbers activated with a stolen telephone – must be restricted to serious crime.

The CJEU decided in October 2018 that access to subscriber information "cannot be defined as 'serious' interference with the fundamental rights of persons" and that access thus may not be limited to cases of serious crime.

9

Consideration 4

- Subscriber information may comprise access numbers, including Internet Protocol addresses, strictly needed to identify a subscriber, such as the first login IP, last login IP or the login IP used at a specific moment in time.
- To be clarified in Explanatory Report of Protocol if necessary (rather than introducing new categories of data).

10

Consideration 5

- A legal requirement for the retention of subscriber information so as to be available for the purposes of specific criminal investigations may be appropriate and proportionate.
- Retention of a limited set of data that does not allow conclusions to be drawn about the content of communications or the everyday habits or social relationships of an individual.

11

Consideration 6

Some jurisprudence/domestic rules distinguish between static and dynamic IP addresses assigned to a specific subscriber

- production of subscriber information related to dynamic IP addresses = interference with the right to the secrecy of communications

However:

- A dynamic – as opposed to a static – IP address is not always linked to a concrete communication
- Linking a dynamic IP address to a specific user by provider may involve automated database query as for static addresses

12

Consideration 7

Access to subscriber information, in relation to both static and dynamic IP addresses, requires a legal basis:

- **Implementation of the production orders of Article 18 Budapest Convention in domestic law.**
- **Lower threshold than search and seizure.**
- **Include specific reference to dynamic IP addresses.**
- **Double door: permission for provider and power to order or request for LEA.**

13

Update: provisional solution in the Protocol

Article [ ] – Direct disclosure of subscriber information

Explanatory report:

"Subscriber information is defined in Article 18.3 of the Convention …."
"… Information needed for the purpose of identifying a subscriber of a service may include certain Internet Protocol (IP) address information – for example, the IP address used at the time when an account was created, the most recent log-on IP address or the log-on IP addresses used at a specific time. In some Parties this information is treated as traffic data for various reasons, including that it is considered to relate to the transmission of a communication. Accordingly, paragraph 9.b provides a reservation for some Parties."

9. A Party may:
a. reserve the right not to apply this Article; or
b. if disclosure of certain types of access numbers under this Article would be inconsistent with the fundamental principles of its domestic legal system, reserve the right not to apply this Article to such numbers.

14

Questions?