



Octopus Conference on Cooperation against Cybercrime WS 4: Transborder access and jurisdiction



1 Justification

- ▶ Do we need transborder access?
- ▶ Do we need common solutions?

2 Current provisions of the Budapest Convention

- ▶ Preservation (16), production orders (18), search/seizure (19), MLA
- ▶ Transborder access (32)

3 Direct LEA transborder access to data

- ▶ Current scenarios & practices

4 Transborder access to data via private sector

- ▶ Current scenarios & practices

5 Implications and concerns

- ▶ Jurisdiction and national sovereignty
- ▶ Data protection, privacy & rule of law safeguards

6 Solutions / options?

alexander.seger@coe.int

1

Justification: the challenge

Key question (Octopus 2010)

- ▶ How to ensure security while maintaining due process, freedom of expression and privacy in a global environment?
- ▶ How to ensure security and privacy in the clouds?

2

Justification: the challenge

The law enforcement challenge

- ▶ LEA need to investigate cybercrime and secure electronic evidence in relation to ANY crime
- ▶ Procedure: Search, seizure, preservation, production of data stored **on a computer system**
- ▶ Rule of law safeguards in country of LEA investigation
- ▶ MLA and provisional measures for international investigations (including safeguards)

3

Justification: the challenge

The law enforcement challenge

- ▶ Search for evidence: where is the computer systems, where is the data?
- ▶ Jurisdiction to enforce?
- ▶ Inefficiency of international cooperation

4

Budapest Convention: LEA access to data

1. Access to data on the territory of the LEA:

- Article 16 – Expedited preservation
- Article 17 – Preservation and partial disclosure
- Article 18 – Production orders
- Article 19 – Search & seizure
- Article 20 – Real-time collection of traffic data
- Article 21 – Interception of content data

Rule of law safeguards

▶ **Article 15**

5

Budapest Convention: LEA access to data

1. Access to data on the territory of the LEA:

- Article 16 – Expedited preservation
- Article 17 – Preservation and partial disclosure
- Article 18 – Production orders
- Article 19 – Search & seizure
- Article 20 – Real-time collection of traffic data
- Article 21 – Interception of content data

▪ **Art. 19 (2): Empower LEA to extend search and seizure to computers accessible from the initial system “in its territory”**

6

Budapest Convention: LEA access to data

2. Access to data on a foreign territory by cooperation with foreign authorities:

▶ Provisional measures

- Article 29/30 – Expedited preservation

▶ Mutual legal assistance

- Article 31 – MLA to access stored data
- Article 33/34 – MLA to collect traffic and intercept content data
- Article 35 – 24/7 Network of contact points

7

Budapest Convention: LEA access to data

3. Access to data on a foreign territory without cooperation of foreign authorities:

▶ Transborder access to stored data

- Article 32a – Publicly available
- Article 32b – With consent

8

Budapest Convention: LEA access to data

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

9

Practices (?): LEA access to data

4. LEA transborder access without consent and without cooperation of foreign authorities

- Art. 19 (2): Empower LEA to extend search and seizure to computers accessible from the initial system [“in its territory”]

**What conditions apply?
Need for common rules?**

10

Practices (?): LEA access to data

5. Access to data on a foreign territory via private sector/ISPs/cloud providers

- Access by LEA to data of foreign natural or legal persons hosted (controlled, processed) on the territory of the law enforcement agency?
- LEA compelling cloud providers/ISPs to provide data hosted/controlled/processed abroad (traffic data, content data, coercive measures/interception)?

Providers in multiple jurisdictions: What rules apply?

What rule of law/human rights safeguards?

Need for common rules?

11

LEA access to data transborder/in the clouds: What options?

1. Make more effective use of Budapest Convention
 - Increase number of parties
 - Provisions on expedited preservation (Art. 16, 17, 29, 30)
 - Provisions on MLA (Art. 31, 33, 34)
 - 24/7 network of contact points (Art. 35)
2. Transborder access under Budapest Convention
3. Identify/negotiate additional international rules or principles for transborder access (including conditions and safeguards) ?
4. Enhance legal certainty for access via providers/private sector
5. Improve data protection systems (Convention 108)

12