Workshop 2: Evidence in the cloud – Criminal justice access to data

Cybercrime Convention Committee (T-CY)

Criminal justice access to data in the cloud: challenges

Discussion paper
prepared by the T-CY Cloud Evidence Group

Strasbourg, 17 June 2015

Alexander Seger
Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

T-CY CEG report: Evidence in the cloud

About the T-CY Cloud Evidence Group:

- Established in December 2014
- Task: To explore solutions for criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance
- Take into account:
  - T-CY assessment on MLA
  - Work of Transborder Group
  - Analysis of challenges
  - Views of industry and other stakeholders
- By December 2016: report with draft options and recommendations for consideration by T-CY

T-CY CEG report: Evidence in the cloud

Purpose of the discussion paper:

To facilitate an exchange of views on current and emerging challenges faced by criminal justice authorities and to seek the cooperation of industry and other stakeholders in identifying solutions.

Such solutions may range from practical measures and documentation of good practices, to guidelines or a binding additional protocol to the Budapest Convention on Cybercrime.

T-CY CEG report: Evidence in the cloud

Cybercrime and the question of electronic evidence:

- Impact of cybercrime ▶ Attacks against core values of societies (human rights, democracy and rule of law)
- Confusion between national security and criminal justice ▶ "We need more effective criminal justice and we need stronger safeguards regarding national security measures."
- Uncertainty regarding the availability of data ▶ no data ▶ no evidence ▶ no justice
- Cloud computing: distributed systems ▶ distributed data ▶ distributed evidence

T-CY CEG report: Evidence in the cloud

Types of data needed for criminal justice purposes:

1. **Subscriber information**
2. **Traffic data**
3. **Content data**

Challenges for criminal justice:

- The scale and quantity of cybercrime, devices, users and victims
- Technical challenges (VPN, P2P, anonymisers, encryption, VOIP, NATs etc.)
- Cloud computing, territoriality and jurisdiction
  - Unclear where data is stored and/or which legal regime applies
  - Service provider under different layers of jurisdiction
  - Unclear which provider for which services controls which data
  - Is data stored or in transit ▶ production orders, search/seizure or interception?
- The challenge of mutual legal assistance

Questions:

Jurisdiction

1. Which government would be the addressee of a lawful request for data by a country attacked in a cloud context where the territorial origin of a cyber offence is not clear, the controller of data is hidden behind layers of service providers, or data is moving, fragmented or mirrored in multiple jurisdictions?

Questions: Jurisdiction

2. What governs jurisdiction to enforce for criminal justice purposes:

a) Location of data?
b) Nationality of owner of data?
c) Location of owner of data?
d) Nationality of data owner?
e) Location of data controller?
f) Headquarters of a cloud service provider?
g) Subsidiary of a cloud service provider?
h) Territory where a cloud provider is offering its services?
i) Laws of the territory where the data owner has subscribed to a service?
j) Territory of the criminal justice authority?

Questions: Jurisdiction

3. What does it mean "offering its services in a territory" (see Article 18.1.b Budapest Convention)?

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

T-CY CEG report: Evidence in the cloud

Questions: Jurisdiction

4. If a domestic court order authorizes the interception of a communication between two nationals or persons on its territory, why would MLA be required even if technically the provider would carry out the interception on a server on a foreign country?

To what extent would the sovereignty of that foreign country be affected?

To what extent would the rights of the defendants not be protected?

Similar for production orders regarding content data?

Questions: Mutual legal assistance

5. Is it realistic that the number of MLA requests sent, received and processed can be increased by a factor of hundred or thousand or ten thousand?

Are governments able to dramatically increase the resources available for the efficient processing of mutual legal assistance requests not only at the level of competent central authorities but also at the level of local courts, prosecution and police offices where MLA requests are prepared and executed

Questions: Mutual legal assistance

6. What would be a reasonable timeframe to obtain data from a foreign authority? Could this be defined in a binding agreement?

Questions: Mutual legal assistance

7. Is it conceivable to develop a light regime for subscriber information, e.g. expedited disclosure?

T-CY CEG report: Evidence in the cloud

Questions: Mutual legal assistance

8. What additional international legally binding solutions could be considered to allow for efficient criminal justice access to specified data in foreign or unknown jurisdictions within the framework of specific criminal investigations? (See T-CY assessment report on MLA)

T-CY CEG report: Evidence in the cloud

Questions: Mutual legal assistance

8. What additional international legally binding solutions

Rec 19 Parties should consider allowing – via legal domestic amendments and international agreement – for the expedited disclosure of the identity and physical address of the subscriber of a specific IP address or user account.

Rec 20 Interested Parties may consider the possibility and scope of an international production order to be directly sent by the authorities of a Party to the law enforcement authorities of another Party.

Rec 21 Parties should consider enhancing direct cooperation between judicial authorities in mutual legal assistance requests.

Questions: Mutual legal assistance

8. What additional international legally binding solutions

Rec 22 Parties may consider addressing the practice of law enforcement and prosecution services obtaining information directly from foreign service providers, and related safeguards and conditions.

Rec 23 Parties should consider joint investigations and/or the establishment of joint investigation teams between Parties.

Rec 24 Parties should consider allowing for requests to be sent in English language. Parties should in particular allow for preservation requests to be sent in English.

Questions: Mutual legal assistance

8. What additional international legally binding solutions

Solutions already available or principles already agreed upon in other international instruments.

For example in the:

- **2nd Additional Protocol on Mutual Legal Assistance in Criminal Matters (ETS 182) of the Council of Europe Convention on Mutual Legal Assistance in Criminal Matters**
- **Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union**
- **European Investigation Order in Criminal Matters of the European Union**