T-CY Cloud Evidence Group

Overview of issues and options currently under consideration by the Cloud Evidence Group

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

1

T-CY Cloud Evidence Group: Rationale

- Budapest Convention: Criminal justice treaty
- Focus on specified data within specific criminal investigations
- Cybercrime AND electronic evidence in relation to any crime
- E-evidence on servers in foreign, unknown, multiple or shifting jurisdictions, in the cloud
- No data, no evidence, no prosecution, no justice, no rule of law
- Less than 1% of cybercrime reported eventually adjudicated = rule of law in cyberspace? = governments meeting obligation to protect (K.U. v Finland)?

2

T-CY Cloud Evidence Group: Rationale

How to ensure the rule of law in cyberspace through more efficient access to electronic evidence for criminal justice purposes?

- Assessment of mutual legal assistance provisions ► 24 recommendations to make MLA more efficient (Dec 2014)
- Transborder access to data (T-CY Transborder Group 2012-2014)
  - Clarification of Article 32b Budapest Convention ► Guidance Note (Dec 2014)
  - Additional options for transborder access ► necessary but politically not feasible in 2014. (Risk of increasing unilateral action)
- T-CY Cloud Evidence Group (2015-2016): Proposals to be submitted to Cybercrime Convention Committee by November 2016

Cloud Evidence Group: Issues identified

- Differentiating subscriber versus traffic versus content data
- Effectiveness of MLA
- Loss of location and transborder access jungle
- Provider present or offering a service in the territory of a Party
- Voluntary disclosure by US-providers
- Emergency procedures
- Data protection

Issue: Subscriber vs traffic vs content data

- Subscriber information most often required in criminal investigations.
- 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.

Issue: Mutual legal assistance

- Mutual legal assistance remains a primary means to obtain electronic evidence for criminal justice purposes
- MLA needs to be made more efficient
- Often subscriber information or traffic data needed first to substantiate or address an MLA request
- MLA often not feasible to secure volatile evidence in unknown or multiple jurisdictions

Issue: "Loss of location"

- In "loss of location" situations (unknown source of attack, servers in multiple or changing locations, live forensics, etc.) MLA not feasible ► principle of territoriality not always applicable
- Direct transborder access to data may be necessary
- What conditions and safeguards?
- Article 32b Budapest Convention limited ► Absence of international legal framework for lawful transborder access
- Unilateral solutions by governments / jungle ► risks to rights of individuals and state to state relations

Issue: "Loss of location"

T-CY Guidance Note on Transborder Access to Data (Article 32), December 2014

Regarding Article 32b, typical situations may include:

"A suspected drug trafficker is lawfully arrested while his/her mailbox - possibly with evidence of a crime - is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b."

Issue: "Loss of location"

Long-arm doctrine of EU anti-trust law (Cases *ICI* 48/69; *Woodpulp* 89/85)

► the European Commission recommends that competition authorities within the European Union obtain access to servers anywhere in the world to gather evidence in anti-trust proceedings:

"To have effective powers to gather digital evidence, it is important that the Authorities can in the exercise of their inspection powers gather digital information which is accessible to the undertaking or person whose premises are being inspected irrespective of where it is stored, including on servers or other storage media located outside the territory of the respective national competition authority or outside the European Union."

Source: European Competition Network "Recommendation on the power to collect digital evidence, including by forensic means"
http://ec.europa.eu/competition/ecn/ecn_recommendation_09122013_digital_evidence_en.pdf

Issue: A service provider offering a service on the territory of a State

- When is a service provider
  - "present" in the territory of a State?
  - "offering a service" in the territory of a State?
- Therefore, when is a service provider subject to a <u>domestic</u> production or other type of coercive order?
- If domestic production orders for subscriber information ► reduction of pressure on MLA system

Issue: "Voluntary" disclosure by private sector entities

- More than 100,000 requests/year by European States to major US providers
- Disclosure of subscriber or traffic data (ca. 60%)
- Providers decide whether or not to respond to lawful requests and whether to notify customers
- Provider policies/practices volatile
- Data protection concerns
- No disclosure by European providers
- No admissibility of data received in some States

► Clearer / more stable framework required

Issue: "Voluntary" disclosure by private sector entities

	Requests for data sent to Apple, Facebook, Google, Microsoft, Twitter and Yahoo in 2015		
Parties	Received	Disclosure	%
Austria	254	119	47%
Belgium	1 992	1 453	73%
Canada	1 157	884	76%
France	27 213	14 746	54%
Germany	29 092	15 469	53%
Italy	7 847	3 591	46%
Netherlands	1 605	1 213	76%
Poland	2 378	820	34%
Portugal	3 255	1 751	54%
Spain	4 151	2 092	50%
United Kingdom	29 937	21 075	70%
USA	89 350	70 116	78%
Total excluding USA	**138 612**	**82 529**	**60%**
Total including USA	227 962	152 644	67%

Issue: Emergency procedures

- Emergency procedures needed to obtain evidence located in foreign jurisdictions through
  - Mutual legal assistance

  and through
  - Direct cooperation with a service provider

Issue: Data protection and other safeguards

- Data protection requirements normally met if powers to obtain data defined in domestic criminal procedure law and/or MLA agreements
- MLA not always feasible
- Increasing "asymmetric" disclosure of data transborder
  - From LEA to service provider ► Permitted with conditions
  - From service provider to LEA ► Unclear legal basis ► providers to assess lawfulness, legitimate interest ► risk of being held liable ▌ Confidentiality requirements

= Clearer framework for public to private to public disclosure transborder required

Cloud Evidence Group: Solutions

Four options to be pursued in parallel:

1. **More efficient MLA**
2. **Guidance Note on Article 18**
3. **Domestic rules on production orders (Article 18)**
4. **Cooperation with providers: practical measures**
5. **Protocol to Budapest Convention**

Solution 1: More efficient MLA

- **Implement legal and practical measures**
  ► Recommendations 1 – 15 of T-CY assessment report on MLA at domestic levels
  - **More resources and training**
  - **Electronic transmission of requests**
  - **Streamlining of procedures**
  - **Etc.**
- **Parties to establish emergency procedures for obtaining data in their MLA systems**
- **Parties to facilitate access to subscriber information in domestic legislation (full implementation of Article 18 Budapest Convention)**

Solution 2: Guidance Note on Article 18

Guidance Note on Article 18 Budapest Convention on production of subscriber information:

- Domestic production orders if a provider is in the territory of a Party even if data is stored in another jurisdiction (Article 18.1.a)
- Domestic production orders for subscriber information if a provider is NOT necessarily in the territory of a Party but is offering a service in the territory of the Party (Article 18.1.b)

Solution 3: Domestic rules for production orders

- Proper implementation of Article 18 at domestic levels
- Lighter regime for production of subscriber information (as compared to traffic and content data)
- Use of information obtained as evidence in criminal proceedings

Solution 4: Cooperation with providers

Pending longer-term solutions:

Practical measures to facilitate transborder cooperation between service providers and criminal justice authorities

- Focus on disclosure of subscriber information upon lawful requests in specific criminal investigations
- Emergency situations
- Consideration of legitimate interests and data protection requirements

Solution 5: Protocol to Budapest Convention

A. Provisions for more efficient MLA

- International production orders
- Simplified MLA for subscriber information
- Direct cooperation between judicial authorities in MLA
- Joint investigations and joint investigation teams
- Requests in English. Audio-video hearings.
- Emergency procedures

B. Provisions for direct cooperation with providers in other jurisdictions

- Disclosure of data by LEA to a service provider abroad in specific situations
- Disclosure of subscriber information by service providers to LEA abroad with conditions and safeguards
- Direct preservation requests to providers abroad
- Admissibility of data obtained directly in domestic proceedings
- Emergency procedures

Solution 5 cont'd: Protocol to Budapest Convention

C. Framework and safeguards for existing practices of transborder access to data

- Transborder access to data with lawfully obtained credentials
- Transborder access in good faith or in exigent circumstances
- The power of disposal as connecting legal factor

D. Data protection

- Requirements for transfer transborder by LEA to a service provider abroad
- Requirements for transfer transborder by a service provider to LEA abroad

NEXT

- Cloud Evidence Group to submit proposals to Cybercrime Convention Committee for consideration (14-15 November 2016)
- Presentation/discussion at Octopus Conference (Strasbourg, 16-18 November 2016)