T-CY Cloud Evidence Group

Exchange of views with data protection organisations

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

Alexander Seger
Executive Secretary
Cybercrime Convention Committee
Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

CEG: Exchange of views with data protection organisations ► Agenda

Introductory presentations:

- Summary of proposals under consideration by Cloud Evidence Group
- Summary of EU data protection package
- Summary of "modernization" proposals related to Convention 108

Discussion of question 1: Implications of the EU DP package and amendments to Convention 108 on Budapest Convention

Discussion of question 2: Disclosure of personal data by LEA to service providers in foreign jurisdictions

Discussion of question 3: Disclosure of personal data by service providers to LEA in foreign jurisdictions

Discussion of question 4: Customer notification

Context: Criminal justice access to evidence in the cloud – options and issues

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
- T-CY Cloud Evidence Group (2015-2016): **issues and options** (Feb 2016 / prov.)

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. Distinction traffic versus subscriber information also unclear in EU legislation.
- Subscriber information held by service providers and obtained through production orders. Lesser interference with 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: A service provider offering a service in 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 domestic 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: 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. **Cooperation with providers: practical measures**
4. **Protocol to Budapest Convention**

Option 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)

Option 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 in the territory of a Party but is offering a service in the territory of the Party (Article 18.1.b)

Question:

Can Article 18.1.b Budapest Convention serve as an international legal basis for the "disclosure by transmission" or "transfer" of subscriber information?

Option 3: 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 or vital interests and data protection requirements**

Option 4: Protocol to Budapest Convention

A. Provisions for more efficient MLA

- International production orders or simplified MLA for subscriber information
- Direct cooperation between judicial authorities in MLA
- Joint investigations and joint investigation teams
- Requests in English
- Emergency procedures

B. Provisions for direct transborder cooperation with providers

- 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

Option 4 cont'd: Protocol to Budapest Convention

C. Framework and safeguards for 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

Criminal justice access to evidence in the cloud

- how to ensure that data protection requirements are met?

New / forthcoming EU instruments

European Union published in the Official Journal (May 2016):

- **Regulation** of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
- **Directive** of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

To be reviewed:

- **Directive on privacy** and electronic communications (2002/58/EC)

Council of Europe instruments

Current

- **Convention** for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108)
- **Additional Protocol** on supervisory authorities and transborder data flows (ETS 181)
- **Recommendation R(87)15** Regulating the use of personal data in the police sector

Forthcoming

- **Amending Protocol to Convention 108** (under negotiation by the ad hoc committee CAHDATA

Update on EU and COE data protection instruments

Discussion of questions 1 - 4

Preliminary question:

"Disclosure by transmission" versus "transfer"

Article 4 GDPR

(2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Chapter V – Transfers of personal data to third countries or international organisations

Preliminary question: What is the logic of Article 48 GDPR?

Chapter V GDPR – Transfers to 3rd countries

Article 48 Transfers or disclosures not authorised by Union law

Data can only be transferred or forwarded to a third country if:

- **the European Commission has adopted an adequacy decision (Article 45),**
- **or appropriate safeguards have been established (Article 46),**
- **or binding corporate rules have been approved (Article 47)**
- **or derogations for specific situations apply (Article 49).**

Preliminary question: What is the logic of Article 48 GDPR?

Article 48 Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Article 49 Derogations for specific situations …

Preliminary question: What is the logic of Article 48 GDPR?

Article 49 Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

….

(d) the transfer is necessary for important reasons of public interest;

(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

…

Question 1

In December 2015, the European Union reached agreement on the substance of a new General Regulation on Data Protection and a Directive on data protection in the criminal justice sector. (Published in the Official Journal in May 2016)

The Amending Protocol to the Council of Europe data protection Convention 108 is about to be finalised.

What are the implications of these new instruments with regard to the Budapest Convention on Cybercrime in its current form?

Re Question 1

EU instruments distinguish between:

1. **"Transfers" of personal data between EU Member States**
2. **"Transfers" from EU Member States to "3rd countries"**
   a) **for which adequacy decisions have been adopted**
   b) **where appropriate safeguards have been established (e.g. in a legally binding instrument)**
   c) **with derogations for specific situations (e.g. protect vital interests, prevention of immediate and serious threats to public security)**

Question 2

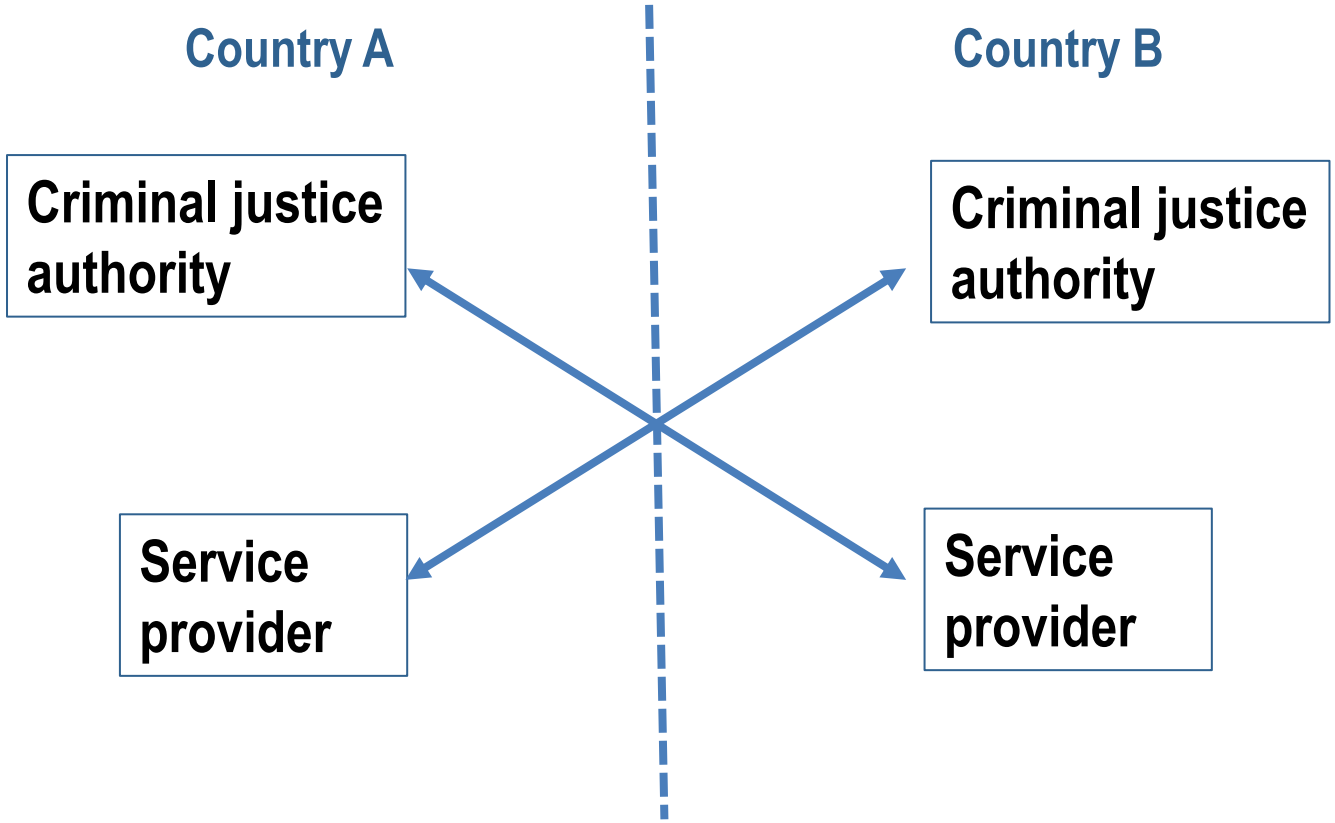
Criminal justice authorities may need to disclose personal data directly to a service provider in another jurisdiction, for example, in situations of imminent danger or other exigent circumstances. This appears to be foreseen in Article 39 of the future EU Directive:

a) Does it make a difference if the service provider is in an EU Member State, or in another Party to Convention 108, or in a third country?

b) Could a Protocol to the Budapest Convention provide a legal basis for such processing? If so, what would be the elements to be foreseen?

NEW c) Could Article 18 Budapest Convention on Production Orders serve as the legal basis for such processing?

Questions 2 + 3 ► Asymmetric “transfers” or “transmissions”



- From Criminal Justice to Service provider: Article 39 EU Directive
- From Service provider to Criminal Justice: ?

Questions 2 + 3 ► "Asymmetric transfers"

Article 39 EU Directive - Transfer of personal data to recipients established in third countries

1. By way of derogation from point (b) of Article 35(1) and without prejudice to any international agreement referred to in paragraph 2 of this Article, Union or Member State law may provide for the competent authorities referred to in point (7)(a) of Article 3, in individual and specific cases, to transfer personal data directly to recipients established in third countries only if the other provisions of this Directive are complied with and all of the following conditions are fulfilled:

   (a) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by Union or Member State law for the purposes set out in Article 1(1);
   (b) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest necessitating the transfer in the case at hand;

Question 2 + 3 ► "Asymmetric transfers"

Article 39 EU Directive - Transfer of personal data to recipients established in third countries

(c) the transferring competent authority considers that the transfer to an authority that is competent for the purposes referred to in Article 1(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;
(d) the authority that is competent for the purposes referred to in Article 1(1) in the third country is informed without undue delay, unless this is ineffective or inappropriate;
(e) the transferring competent authority informs the recipient of the specified purpose or purposes for which the personal data are only to be processed by the latter provided that such processing is necessary.

2. An international agreement referred to in paragraph 1 shall be any bilateral or multilateral international agreement in force between Member States and third countries in the field of judicial cooperation in criminal matters and police cooperation.

Question 3

Criminal justice authorities increasingly send requests for subscriber information (and sometimes also for other data) directly to service providers in other jurisdictions, and often service provider respond positively to such requests. In emergency situations, including situations of child abuse, service providers are sometimes also prepared to disclose content information:

a) What would be the basis or reasoning under European data protection instruments and/or domestic law permitting such disclosure directly transborder in non-emergency situations?

b) What would be the basis or reasoning under European data protection instruments and/or domestic law permitting such disclosure, including of content, directly transborder in emergency situations?

c) Does it make a difference if the receiving criminal justice authority is in an EU M/S or adequate country or territory, or in another Party to Convention 108 or in a 3rd country?

d) Could a Protocol to the Budapest Convention provide a legal basis for such processing? If so, what would be the elements to be foreseen?

Question 3 e):

Can Article 18.1.b Budapest Convention serve as an international legal basis for the "disclosure by transmission" or "transfer" of subscriber information?

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 in the territory of a Party but is offering a service in the territory of the Party (Article 18.1.b)

Question 4

Service providers receiving requests for data from criminal justice authorities in another jurisdiction may notify their customer of such request.

Customer notification may harm investigations or witnesses or threaten the safety of requesting law enforcement officials.

Is customer notification a requirement under data protection instruments (e.g. under Article 14 of the future General Data Protection Regulation)?

Question 4 ► Customer notification

1. On someone's [Social Media Account], we see that someone writes in the name of ISIS that [CITY] will be attacked on [DATE]
2. We also found these postings on the [Social Media Account]
3. [Social Media Provider] disclosed subscriber and login information based on our emergency request. So far so good.
4. We could see that there's a [Webmail] email connected to that [Social Media Account].
5. So, in order to have more information, I did a similar request to [Webmail provider].
6. They sent me their new policy where they write clearly that also for imminent physical threat procedures they have the right to advise their client.

Question 4 ► Customer notification

7. So we asked for more clarification... "ONE QUESTION ABOUT THE [Webmail Provider] DISCLOSURE POLICY: WHAT INFORMATION ABOUT THE REQUESTER WOULD YOU PROVIDE TO THE ACCOUNT HOLDER? WOULD IT BE SOMETHING RELATIVELY GENERAL LIKE "THE AUTHORITIES OF [COUNTRY]" OR WOULD YOU DISCLOSE THE ACTUAL NAME AND EMAIL ADDRESS OF THE PERSON WHO SIGNED THE EMERGENCY DISCLOSURE REQUEST. WE WOULD LIKE TO KNOW THIS AS THIS MAY MEAN THAT A POTENTIAL TERRORIST MAY RECEIVE PERSONAL INFORMATION OF A LAW ENFORCEMENT OFFICER.

8. They called me back, telling me that they understand the situation, but they cannot guarantee that after 90 days my contact information won't be given to the client.

Conclusion:

Criminal justice access to evidence in the cloud: how to ensure that data protection requirements are met?

Article 18 (Production order) as legal basis for disclosure of subscriber information by service providers?

What DP provisions should a Protocol foresee?